

AutoCSP: Automatically Retrofitting CSP to Web Applications

Mattia Fazzini, Prateek Saxena, Alessandro Orso



Web Applications

Web Applications

The New York Times

Web Applications

The New York Times

amazon.com[®]

Web Applications

The New York Times

You  Tube

amazon.com[®]

Web Applications

The New York Times

You  Tube

amazon.com[®]

facebook[®]

Web Applications

淘宝网
Taobao.com

twitter 

 腾讯网
QQ.com

PayPal™

Baidu 百度 

The New York Times

YAHOO!®

 新浪网
sina.com.cn

GitHub

You Tube 

Google

amazon.com® 

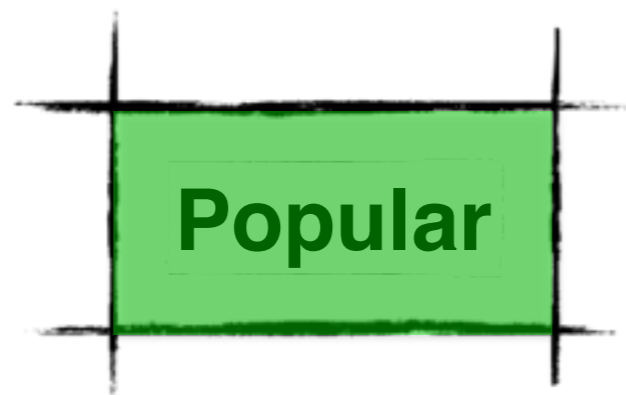
 Windows Live™

Linked in™ 

facebook®

WIKIPEDIA

Web Applications



Web Applications

淘宝网
Taobao.com

twitter

腾讯网
QQ.com

PayPal™

Baidu 百度

The New York Times

YAHOO!

sina 新浪网
sina.com.cn

GitHub

You Tube

Google

amazon.com

Windows Live

LinkedIn

facebook

WIKIPEDIA

Popular

Target

Cross-Site Scripting (XSS)



Cross-Site Scripting (XSS)



Hydara et. al., 2014

XSS Publications



Cross-Site Scripting (XSS)

18 Sep 2014

“eBay Under Fire After Cross Site Scripting Attack”

16 Sep 2013

“NASDAQ Website Vulnerable to XSS Attacks”

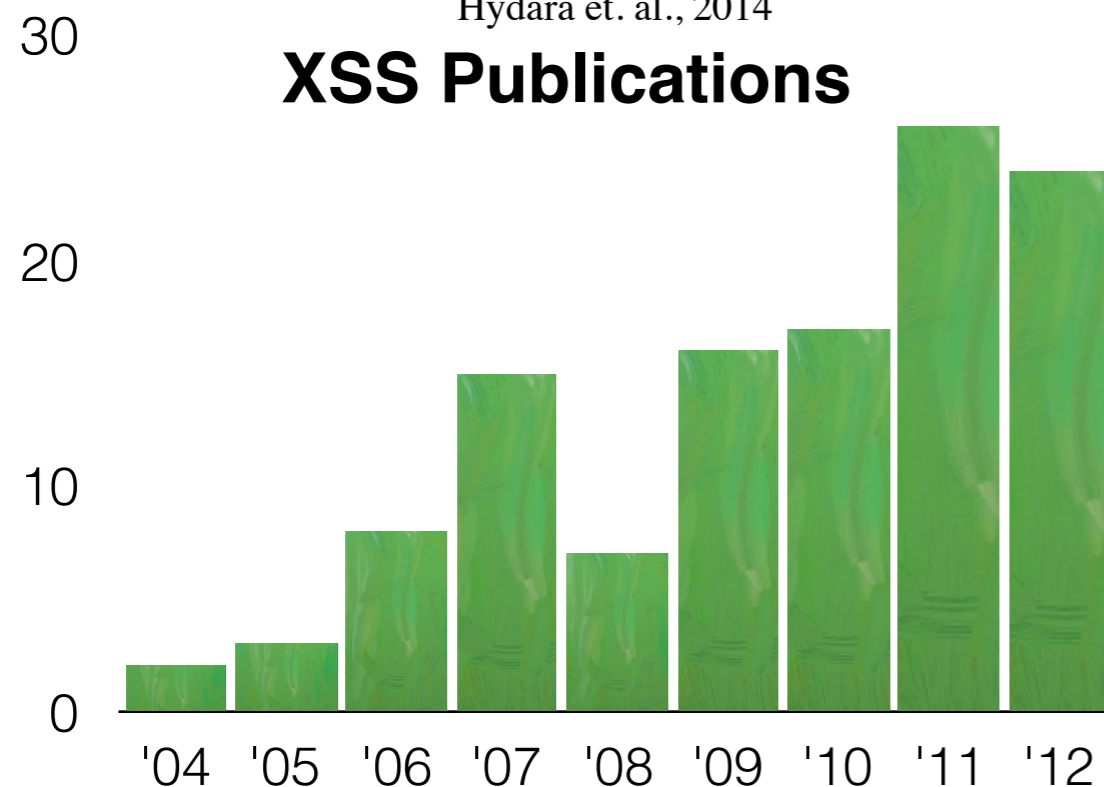
28 May 2013

“PayPal vulnerable to cross-site scripting again”



Hydara et. al., 2014

XSS Publications

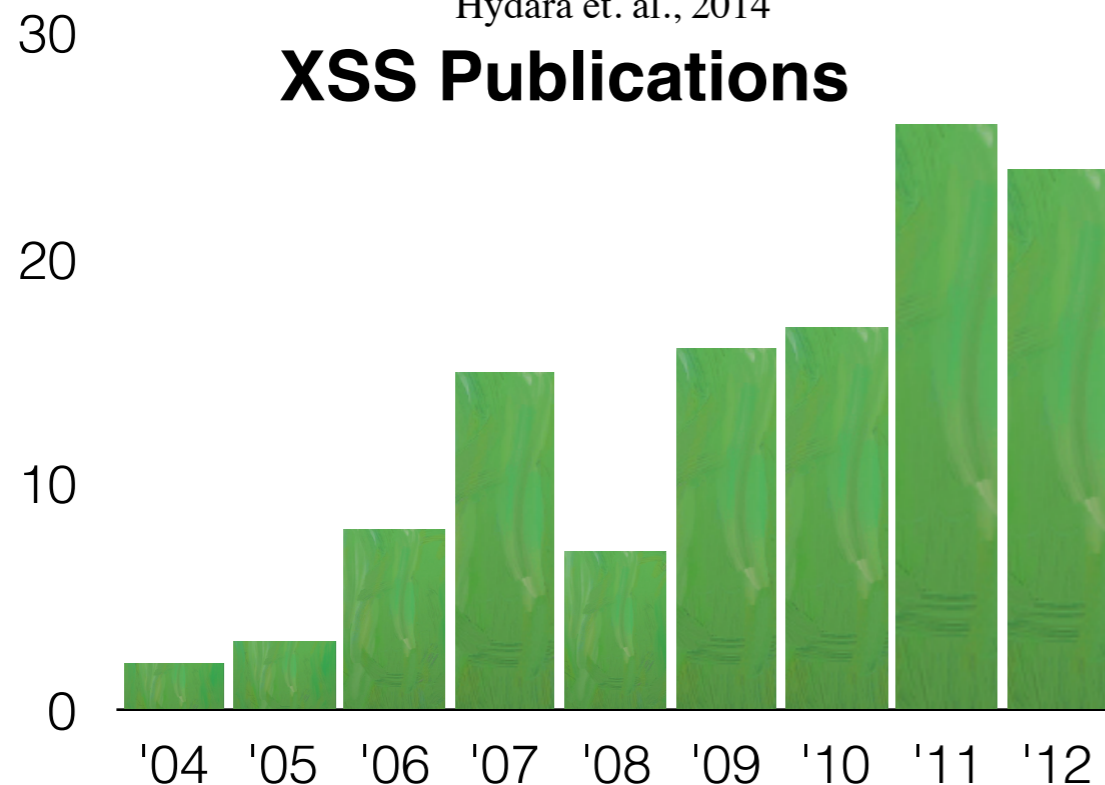


Cross-Site Scripting (XSS)



Hydara et. al., 2014

XSS Publications



18 Sep 2014

“eBay Under Fire After Cross Site Scripting Attack”

16 Sep 2013

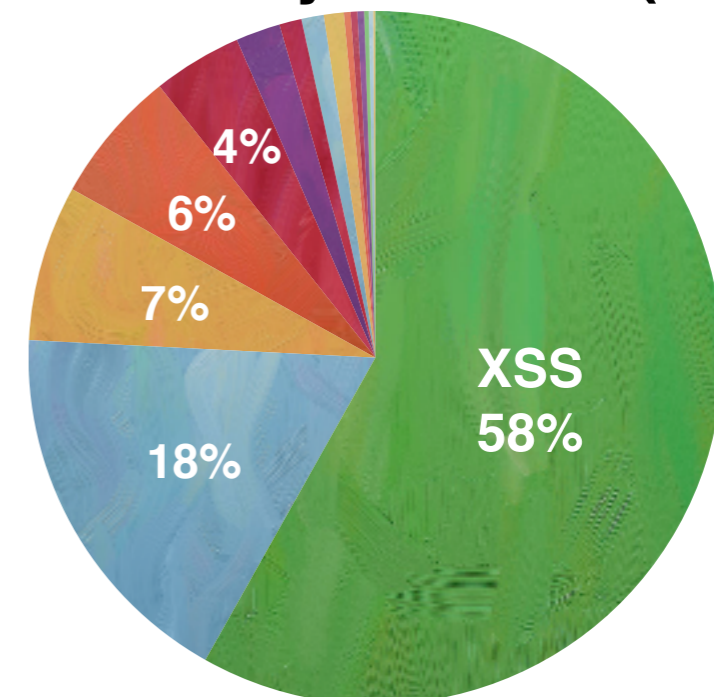
“NASDAQ Website Vulnerable to XSS Attacks”

28 May 2013

“PayPal vulnerable to cross-site scripting again”

WhiteHat Security, 2014

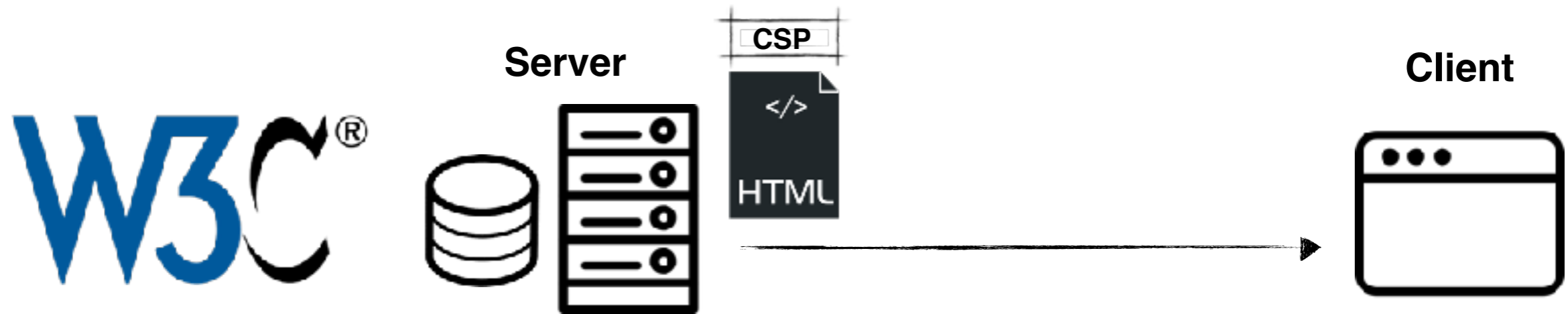
Vulnerability Classes (2014)



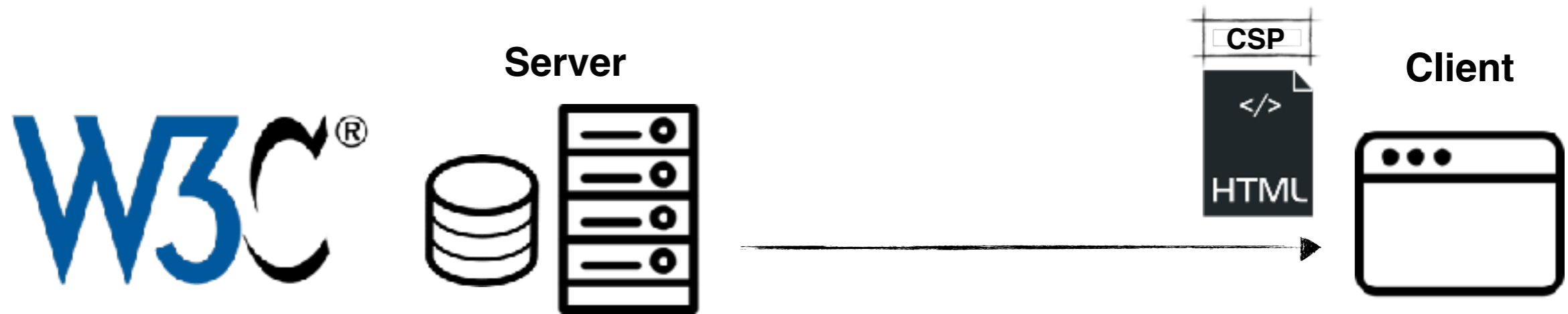
Content Security Policy (CSP)



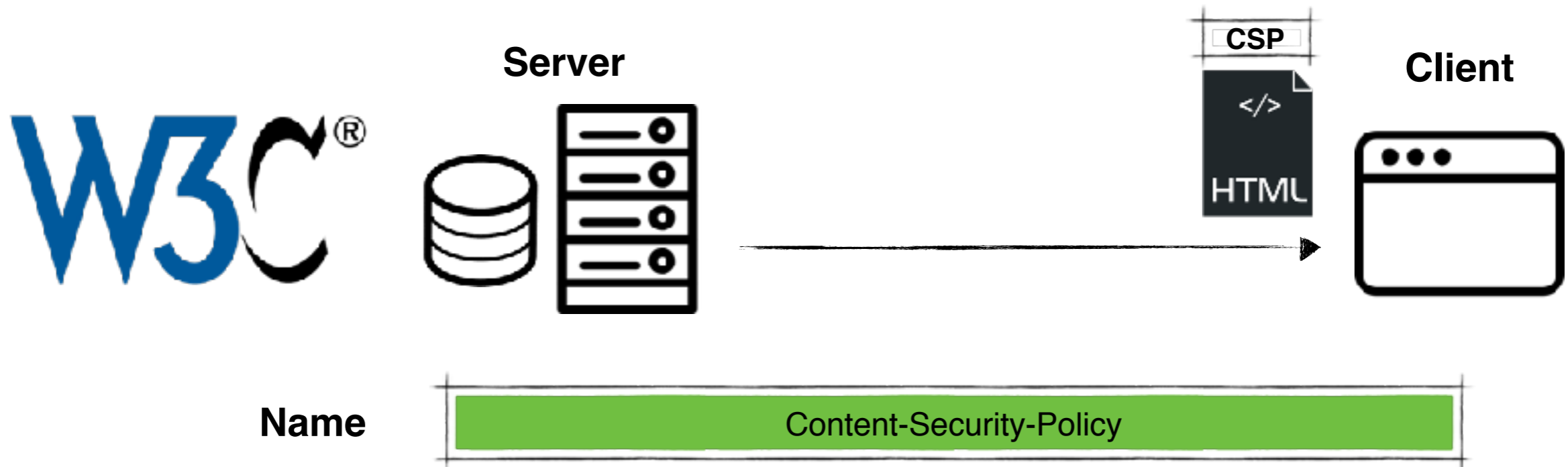
Content Security Policy (CSP)



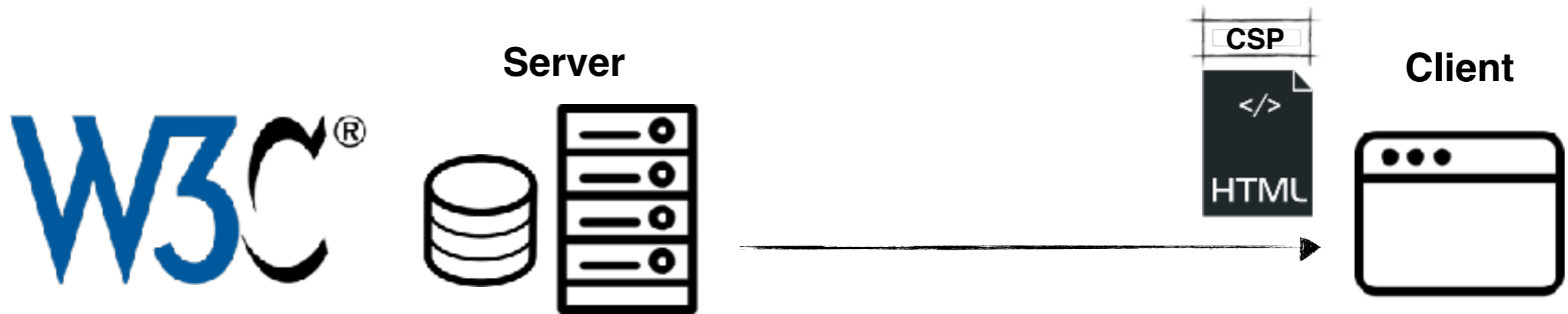
Content Security Policy (CSP)



Content Security Policy (CSP)



Content Security Policy (CSP)



Name

Content-Security-Policy

Directives

script-src

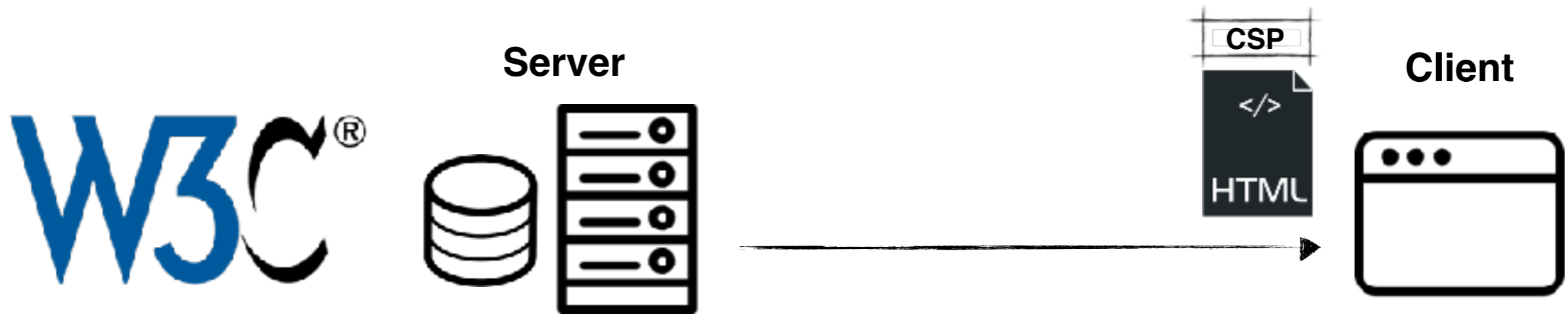
style-src

img-src

frame-src

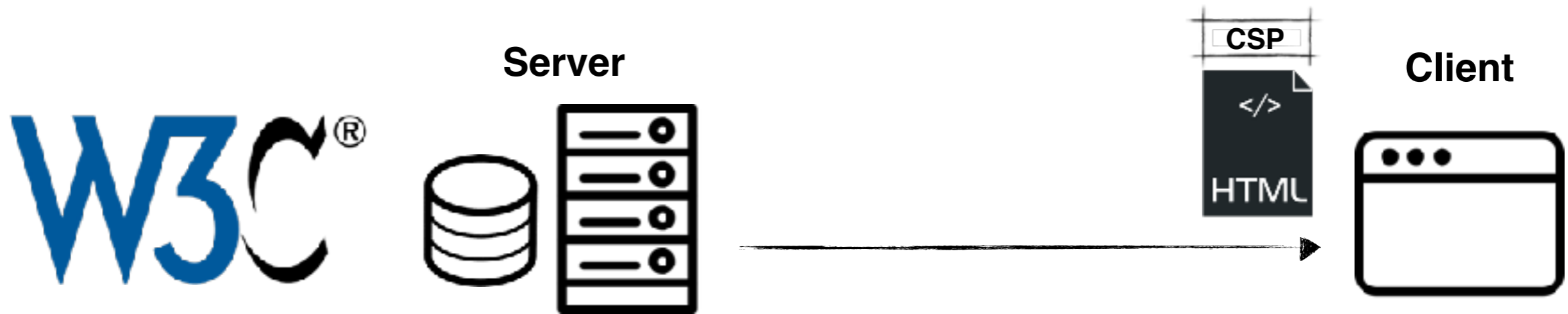
...

Content Security Policy (CSP)



Name	Content-Security-Policy				
Directives	script-src	style-src	img-src	frame-src	...
Values	'none', 'self', domain, 'unsafe-inline', 'unsafe-eval'				

Content Security Policy (CSP)



Name	Content-Security-Policy				
Directives	script-src	style-src	img-src	frame-src	...
Values	'none', 'self', domain, 'unsafe-inline', 'unsafe-eval'				



v13



v42



v47



v9



v33

Content Security Policy (CSP)

Server

CSP

Client

Facebook website screenshot. The developer tools Network tab shows the response headers for the main document. The CSP header is highlighted in red:

```
cache-control: private, no-cache, no-store, must-revalidate  
content-encoding: gzip  
content-security-policy: default-src *; script-src https://*.facebook.com http://*.facebook.com http://*.fbcdn.net http://*.fbcdn.net *.facebook.net *.google-analytics.com *.virtualsearth.net *.google.com 127.0.0.1:* *.spotilocal.com; 'unsafe-inline' 'unsafe-eval' https://*.akamaihd.net http://*.akamaihd.net *.atlassolutions.com chrome-extension://lifbciblhhkdhocfpjfnlhfpfnpldfl; style-src * 'unsafe-inline'; connect-src https://*.facebook.com http://*.facebook.com https://*.fbcdn.net http://*.fbcdn.net *.facebook.net *.spotilocal.com; https://*.akamaihd.net wss://*.facebook.com; wss://*.facebook.com; http://*.akamaihd.net https://fb.scanandcleanlocal.com; *.atlassolutions.com http://attachment.fsbx.com https://attachment.fsbx.com;
```

GitHub website screenshot. The developer tools Network tab shows the response headers for the main document. The CSP header is highlighted in red:

```
Cache-Control: no-cache  
Content-Encoding: gzip  
Content-Security-Policy: default-src *; script-src assets-cdn.github.com collector-cdn.github.com; object-src assets-cdn.github.com; style-src 'self' 'unsafe-inline' 'unsafe-eval' assets-cdn.github.com; img-src 'self' data: assets-cdn.github.com identities.github.com www.google-analytics.com collector.githubapp.com *.githubusercontent.com *.gravata.com *.wp.com; media-src 'none'; frame-src 'self' render.githubusercontent.com gist.github.com www.youtube.com player.vimeo.com checkout.paypal.com; font-src assets-cdn.github.com; connect-src 'self' live.github.com wss://live.github.com uploads.github.com status.github.com api.github.com www.google-analytics.com github-cloud.s3.amazonaws.com  
Content-Type: text/html; charset=utf-8  
Date: Tue, 28 Apr 2015 18:02:54 GMT
```

Twitter website screenshot. The developer tools Network tab shows the response headers for the main document. The CSP header is highlighted in red:

```
cache-control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0  
content-encoding: gzip  
content-length: 17253  
content-security-policy: default-src https;; connect-src https;; font-src https: data;; frame-src https: twitter;; img-src https: data;; media-src https;; object-src https;; script-src 'unsafe-inline' 'nonce-nFt6KByA1StGfQotsDdQyw=' 'unsafe-eval' https;; style-src 'unsafe-inline' https;; report-uri https://twitter.com/i/csp_report?a=NYQWCYLXFYZK0ZLGD0%3D%3D%3D%3D%3D%3D%3D&ro=false;  
content-type: text/html; charset=utf-8  
date: Tue, 28 Apr 2015 18:03:56 GMT  
expires: Tue, 31 Mar 1981 05:00:00 GMT  
last-modified: Tue, 28 Apr 2015 18:03:56 GMT  
ms: A
```



v13

v42

v47

v9

v33

Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15 href='javascript:grades();'>
16 Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```

Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15 href='javascript:grades();'>
16 Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```

Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11   }
12 </script>
13 ...
14 <a
15 href='javascript:grades();'>
16   Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```



Motivating Example


Server-side Code


```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15 href='javascript:grades();'>
16 Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```

 Hardcoded inline script

 Hardcoded JS scheme

 Hardcoded inline attribute

Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```



Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15 href='javascript:grades();'>
16 Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```



Inline script from persistent XSS



Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15 href='javascript:grades();'>
16 Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```

Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
```

Content-Security-Policy:
script-src: 'none'
style-src: 'none'

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15   href='javascript:grades();'>
16   Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```

Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
```

Content-Security-Policy:
script-src: 'none'
style-src: 'none'

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15   href='javascript:grades();'>
16   Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```



Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
```

Content-Security-Policy:
script-src: 'none'
style-src: none

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15   href='javascript:grades();'>
16   Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```



Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15 href='javascript:grades();'>
16 Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```

Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
```

Content-Security-Policy:
script-src: 'unsafe-inline'
style-src: 'unsafe-inline'

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15   href='javascript:grades();'>
16   Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```


Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
```

Content-Security-Policy:
script-src: 'unsafe-inline'
style-src: 'unsafe-inline'

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15   href='javascript:grades();'>
16   Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```



Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
```

Content-Security-Policy:
script-src: 'unsafe-inline'
style-src: 'unsafe-inline'

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15   href='javascript:grades();'>
16   Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```



Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

Web Page

```
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8   function grades(){
9     document.student.page2.value=3;
10    document.student.submit();
11  }
12 </script>
13 ...
14 <a
15 href='javascript:grades();'>
16 Grades
17 </a>
18 ...
19 <td style='text-align: left;'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```




Motivating Example

Server-side Code


```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

CSP-enabled Web Page

Legend:

-  Inline script to external script
-  Inline to external script
-  Inline attribute to external style

```
1 <html>
2 <head>
3 ...
4 <script src='uri.js'>
5 </script>
6 <link rel='stylesheet'
7   type='css' href='style.css'/>
8 ...
9 </head>
10 <body>
11 ...
12 <script src='external.js'>
13 </script>
14 ...
15 <a id='uri' href='#'>
16   Grades
17 </a>
18 ...
19 <td id='style'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```

 XSS inline script

Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
```

Content-Security-Policy:
script-src: 'domain'
style-src: 'domain'

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

CSP-enabled Web Page

```
1 <html>
2 <head>
3 ...
4 <script src='uri.js'>
5 </script>
6 <link rel='stylesheet'
7   type='css' href='style.css'/>
8 ...
9 </head>
10 <body>
11 ...
12 <script src='external.js'>
13 </script>
14 ...
15 <a id='uri' href='#'>
16   Grades
17 </a>
18 ...
19 <td id='style'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```

Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
```

Content-Security-Policy:
script-src: 'domain'
style-src: 'domain'

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

CSP-enabled Web Page

```
1 <html>
2 <head>
3 ...
4 <script src='uri.js'>
5 </script>
6 <link rel='stylesheet'
7   type='css' href='style.css'/>
8 ...
9 </head>
10 <body>
11 ...
12 <script src='external.js'>
13 </script>
14 ...
15 <a id='uri' href='#'>
16   Grades
17 </a>
18 ...
19 <td id='style'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```



Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
```

Content-Security-Policy:
script-src: 'domain'
style-src: 'domain'

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

CSP-enabled Web Page

```
1 <html>
2 <head>
3 ...
4 <script src='uri.js'>
5 </script>
6 <link rel='stylesheet'
7   type='css' href='style.css'/>
8 ...
9 </head>
10 <body>
11 ...
12 <script src='external.js'>
13 </script>
14 ...
15 <a id='uri' href='#'>
16   Grades
17 </a>
18 ...
19 <td id='style'>
20   <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```



Motivating Example

Server-side Code

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9
```

CSP-enabled Web Page

```
1 <html>
2 <head>
3 ...
4 <script src='uri.js'>
5 </script>
6 <link rel='stylesheet'
7   type='css' href='style.css'/>
8 ...
9 </head>
```

Goal

Automatically change server-side code to generate CSP-enabled web pages

```
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

```
15 <a id='uri' href='#'>
16 Grades
17 </a>
18 ...
19 <td id='style'>
20 <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```


AutoCSP Overview

AutoCSP Overview

Inputs



Web App

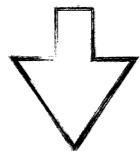


AutoCSP Overview

Inputs



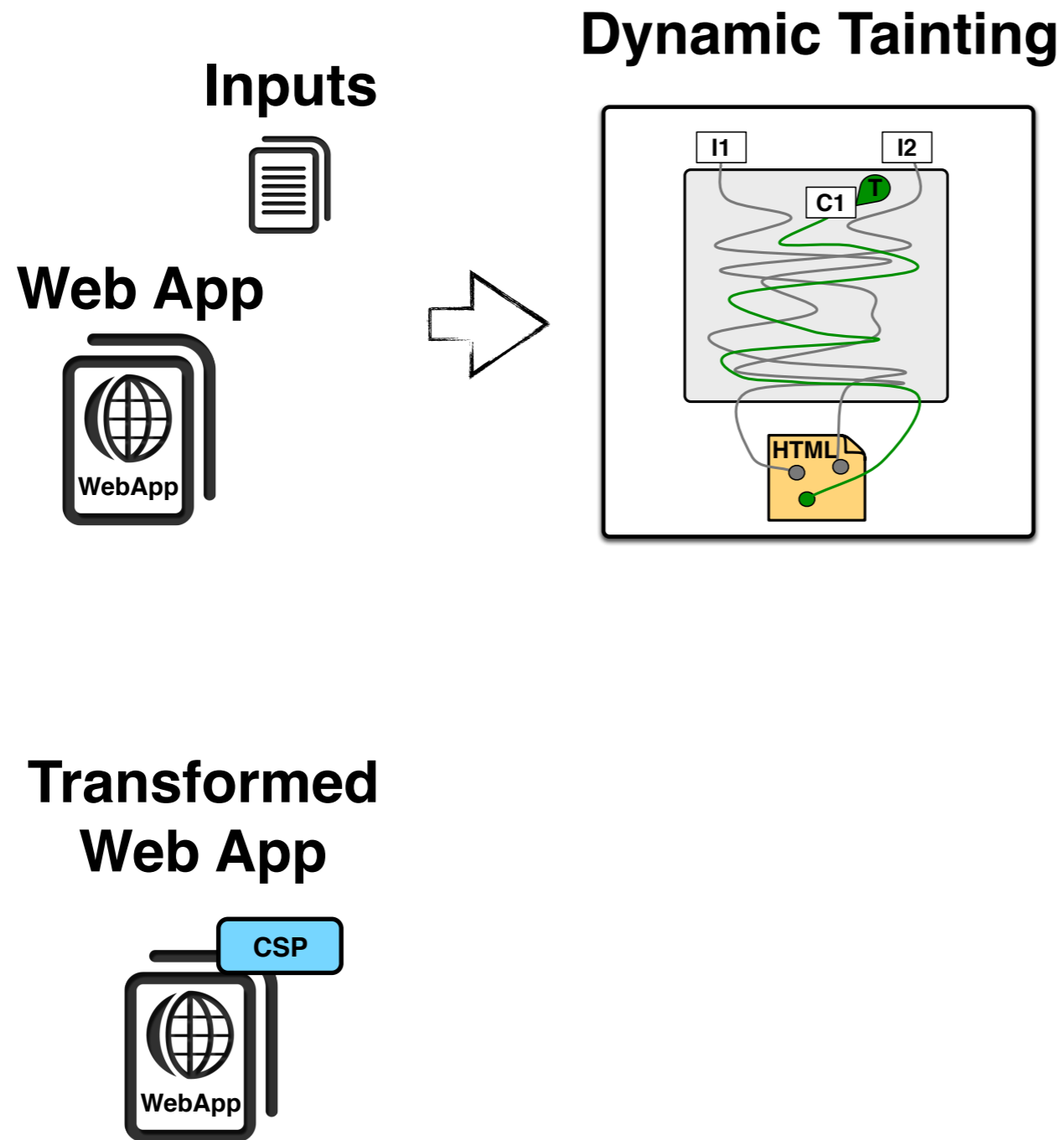
Web App



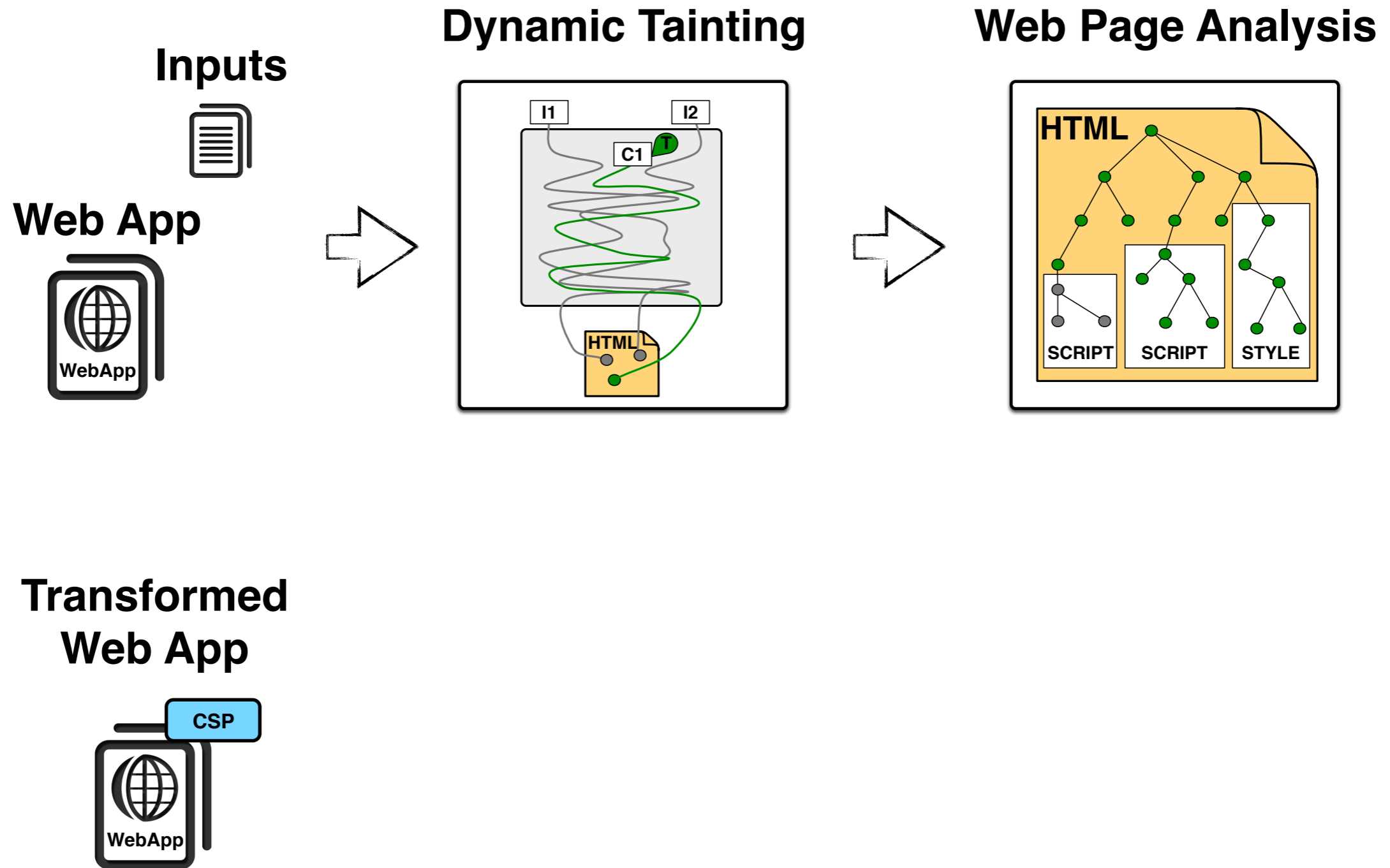
Transformed
Web App



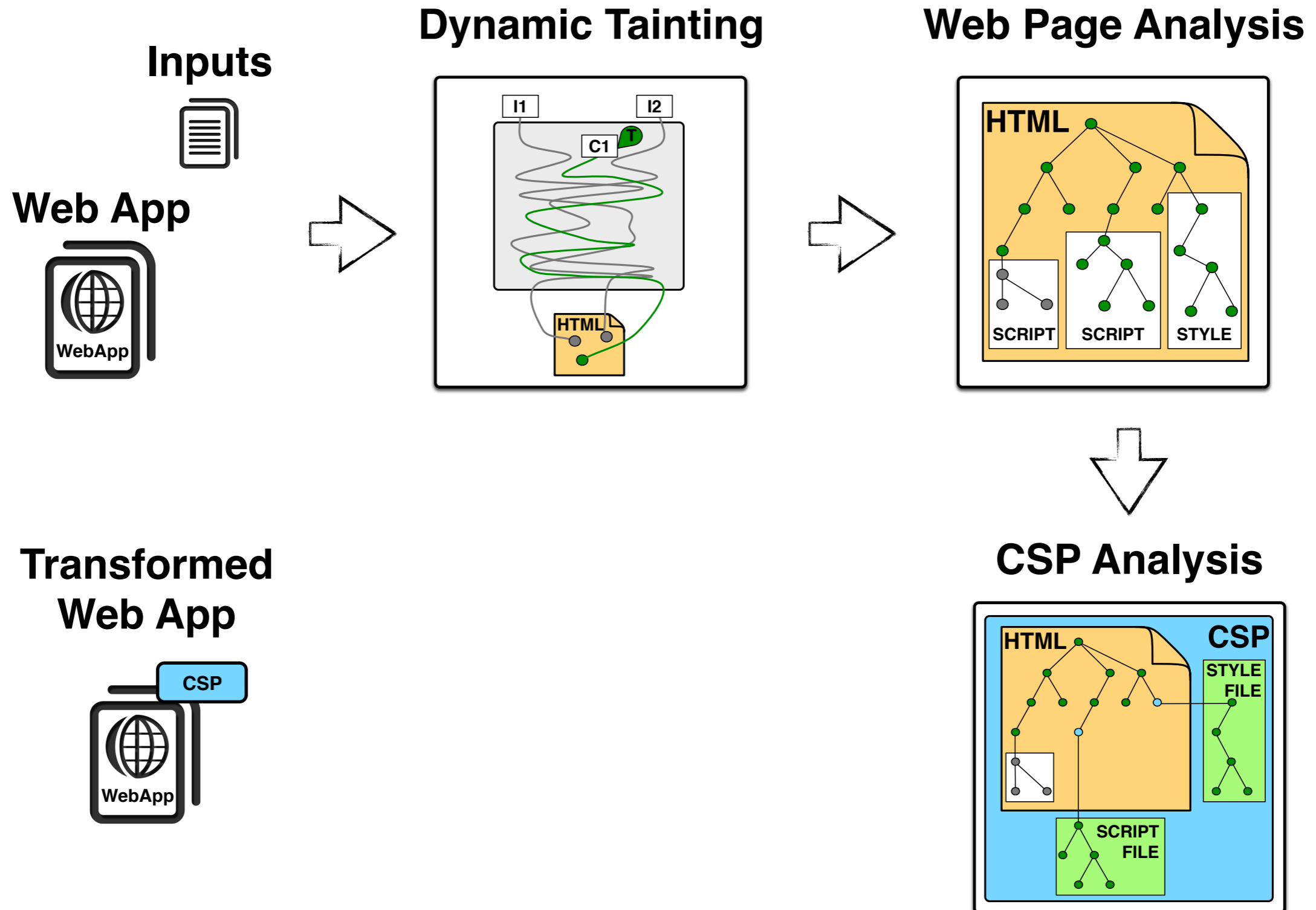
AutoCSP Overview



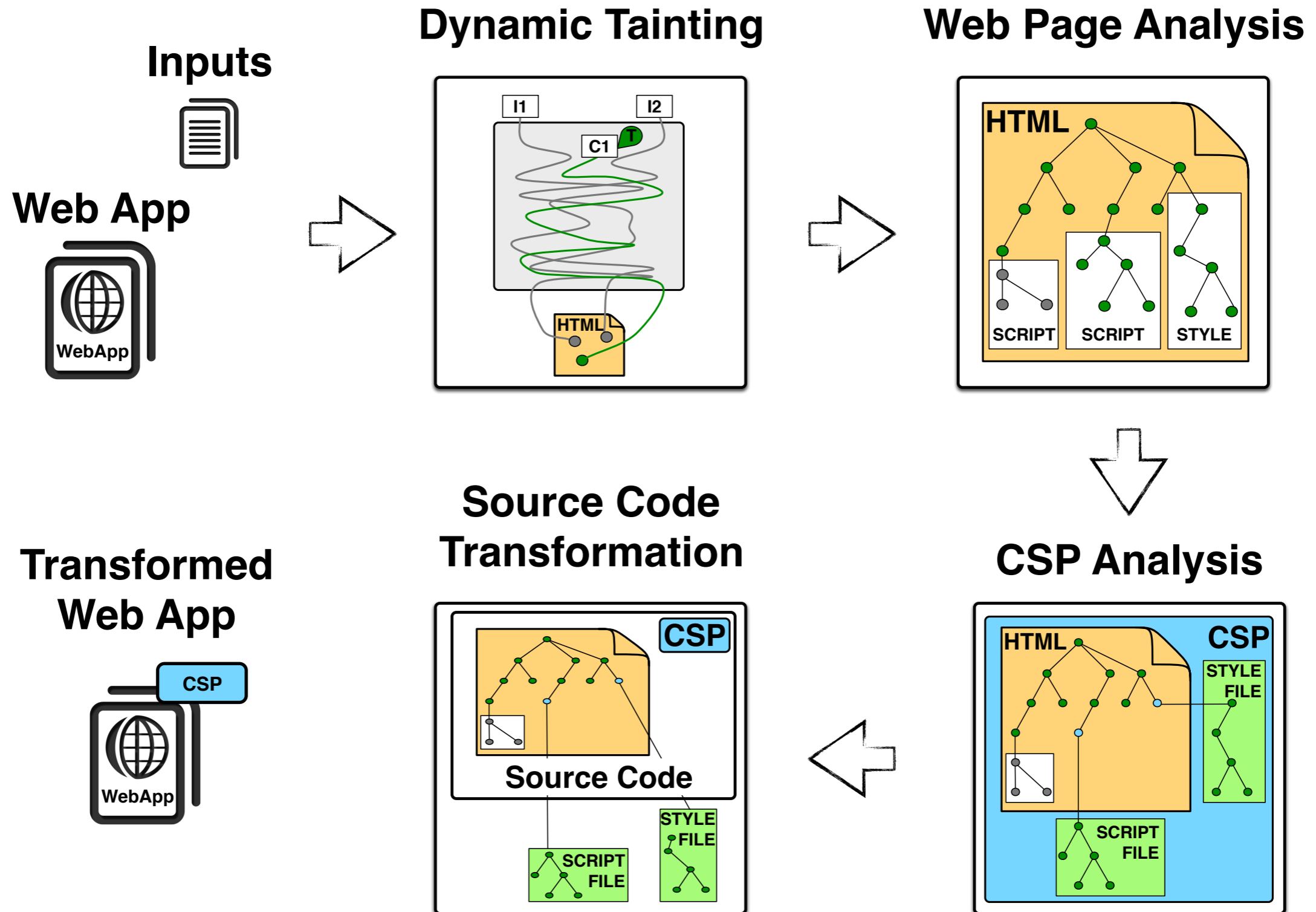
AutoCSP Overview



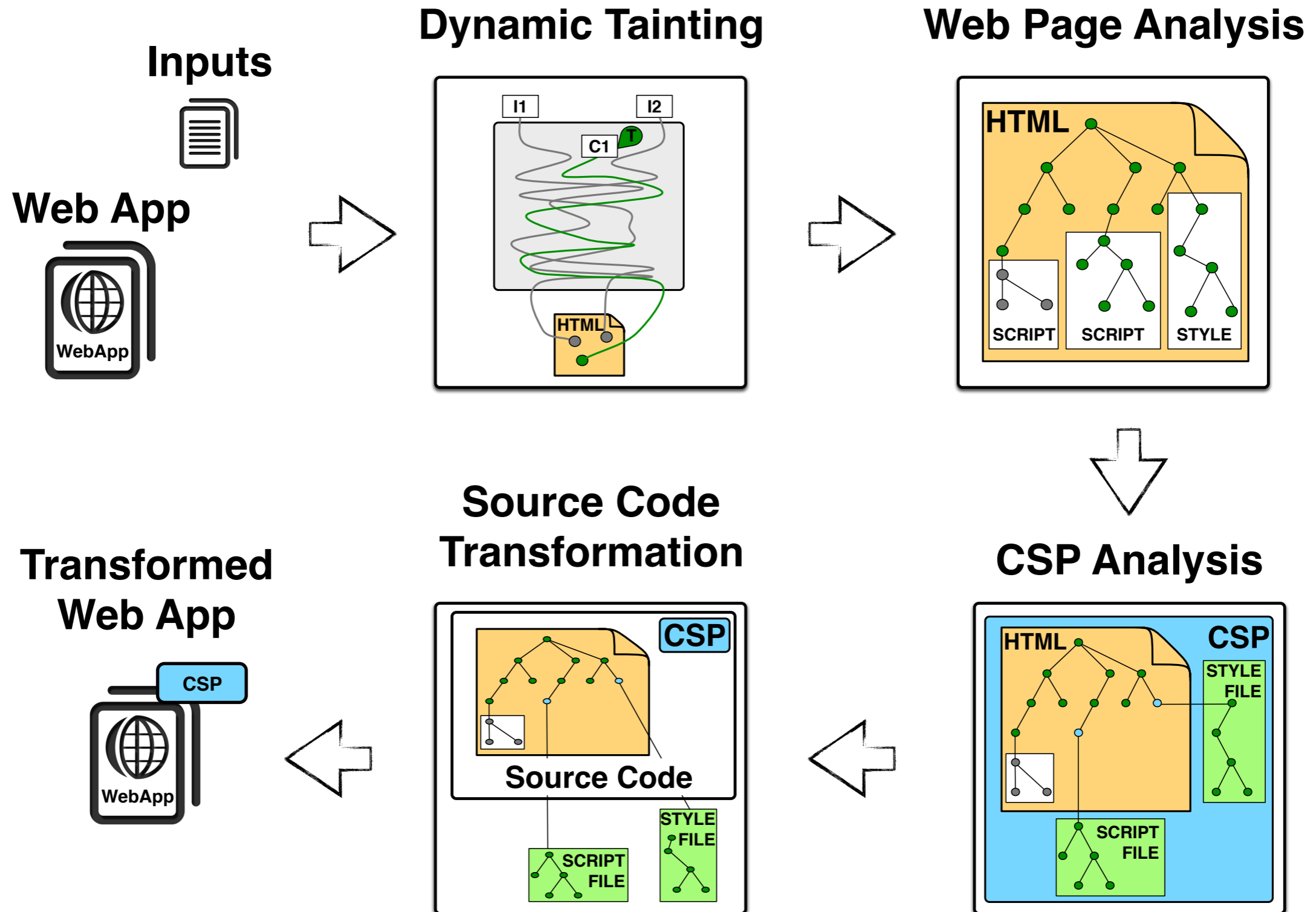
AutoCSP Overview



AutoCSP Overview

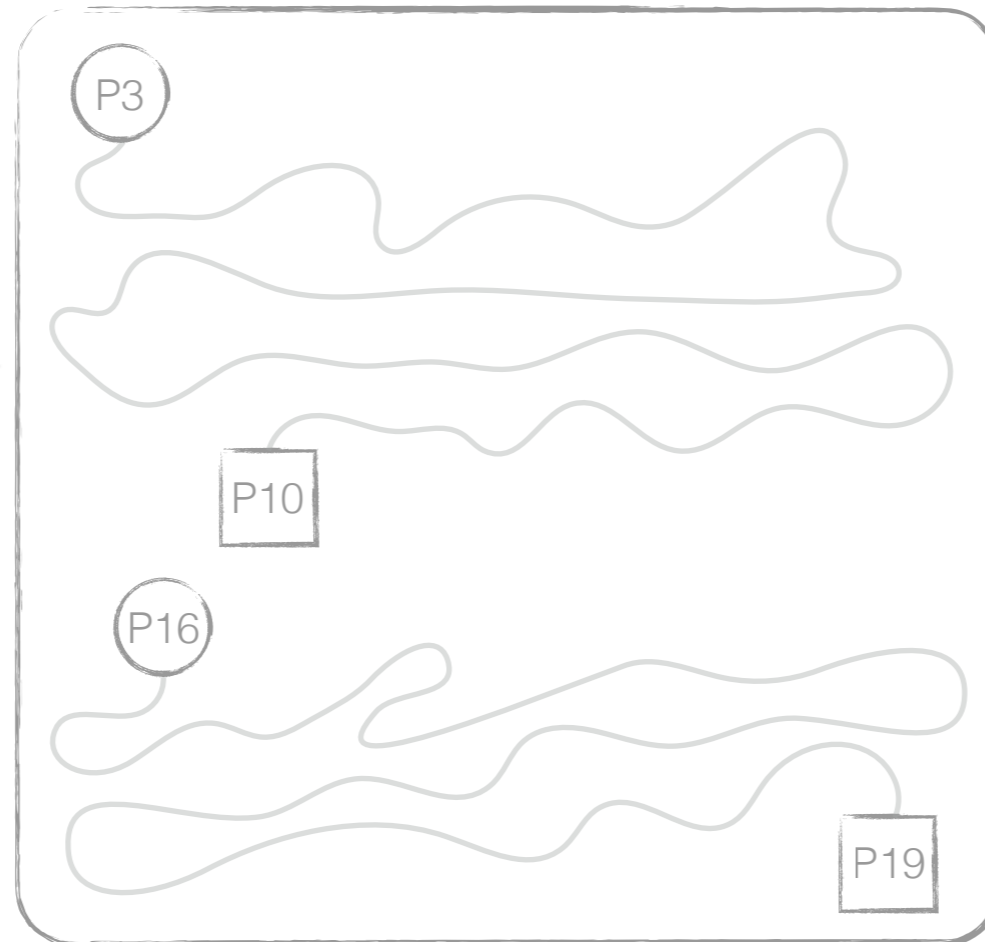


AutoCSP Overview



(1) Dynamic Tainting

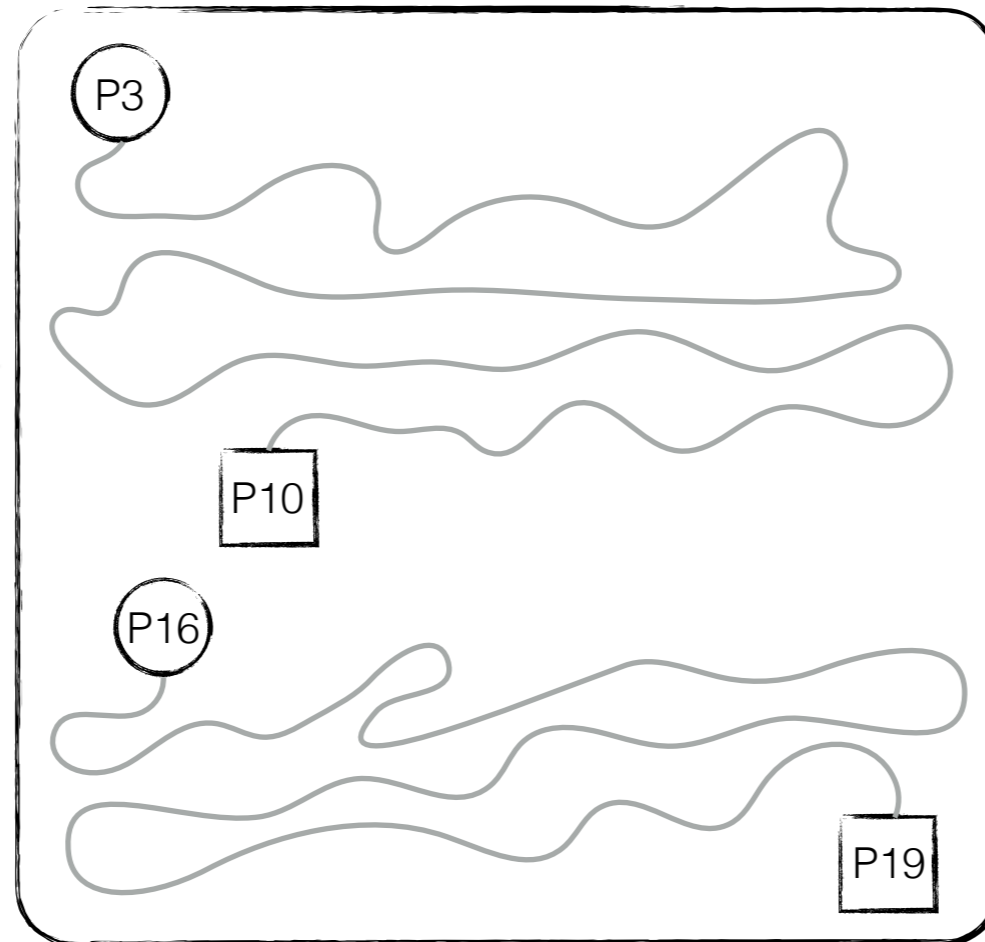
Positive Dynamic Tainting



```
...
3 $out("<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
...
10 print($out);
...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
```

(1) Dynamic Tainting

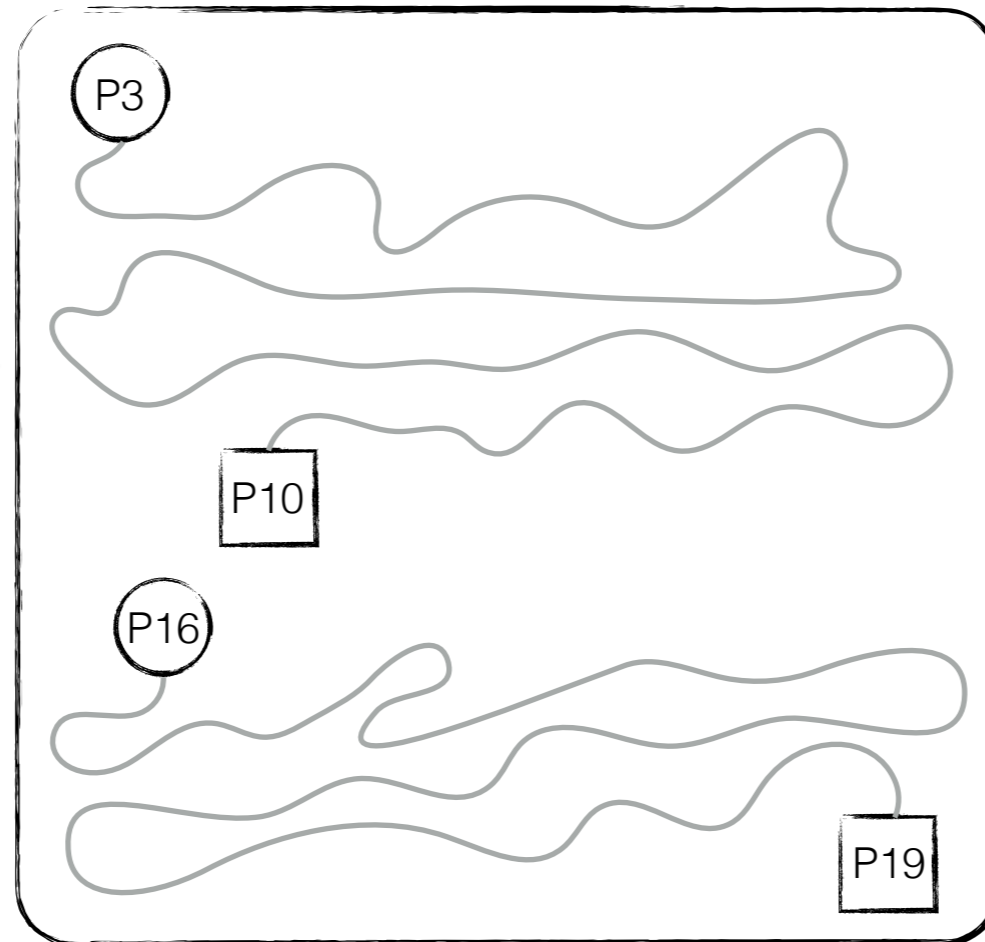
Positive Dynamic Tainting



```
...
3 $out("<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
...
10 print($out);
...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
```

(1) Dynamic Tainting

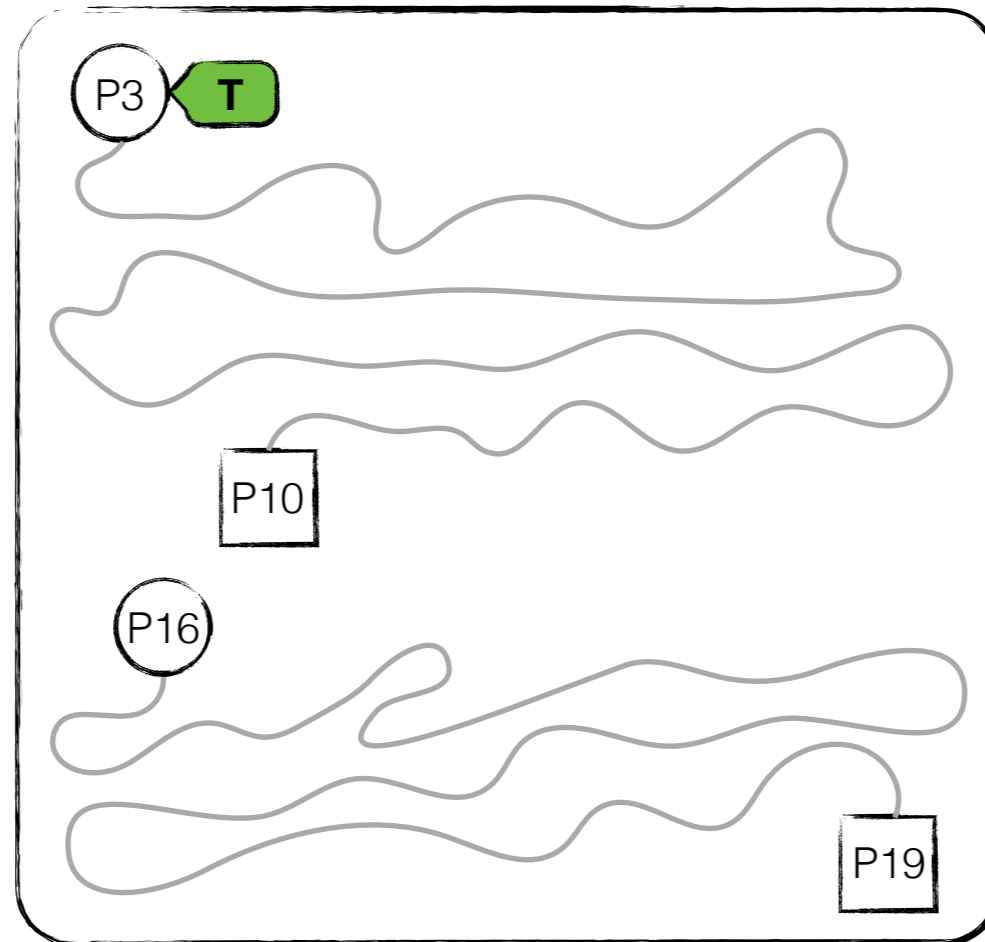
Positive Dynamic
Tainting



```
...  
3 $out="<script>  
4 function grades(){  
5   document.student.page2.value=3;  
6   document.student.submit();  
7 }  
8 </script>"  
...  
10 print($out);  
...  
16 while($assignment =  
17 mysql_fetch_row($query)){  
18 ...  
19 print("<td style='text-align:left;'>"  
20   .$assignment[5].  
21   "</td>");
```

(1) Dynamic Tainting

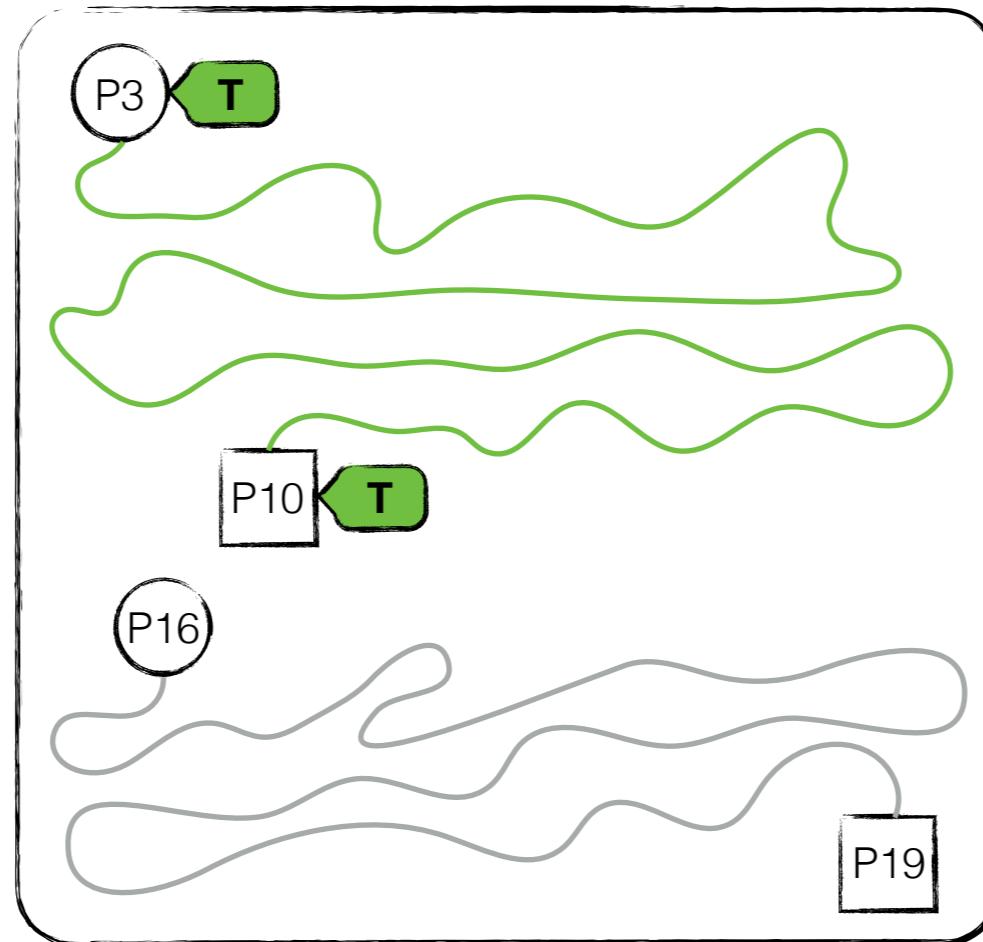
Positive Dynamic Tainting



```
...  
3 $out("<script>  
4 function grades(){  
5   document.student.page2.value=3;  
6   document.student.submit();  
7 }  
8 </script>"  
...  
10 print($out);  
...  
16 while($assignment =  
17 mysql_fetch_row($query)){  
18 ...  
19 print("<td style='text-align:left;'>"  
20   .$assignment[5].  
21   "</td>");
```

(1) Dynamic Tainting

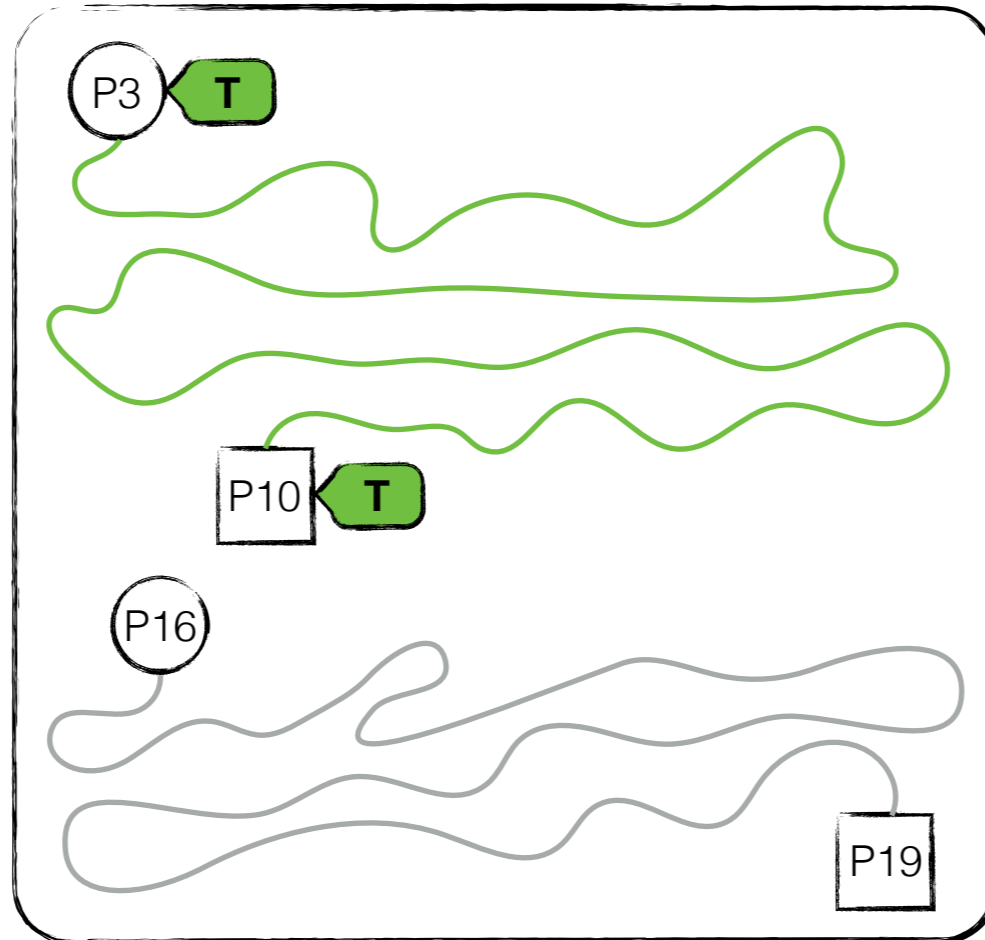
Positive Dynamic Tainting



```
...  
3 $out("<script>  
4 function grades(){  
5   document.student.page2.value=3;  
6   document.student.submit();  
7 }  
8 </script>"  
...  
➔ 10 print($out);  
...  
16 while($assignment =  
17 mysql_fetch_row($query)){  
18 ...  
19 print("<td style='text-align:left;'>"  
20   .$assignment[5].  
21   "</td>");
```

(1) Dynamic Tainting

Positive Dynamic Tainting

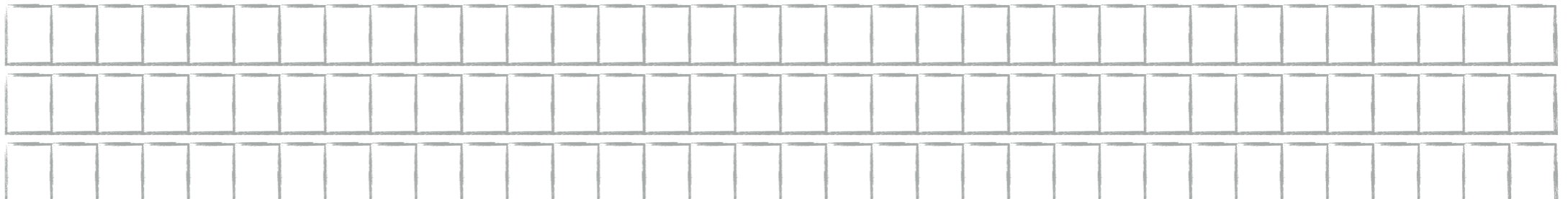


```
...
3 $out("<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
...
➔ 10 print($out);
...
16 while($assignment =
17   mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     . $assignment[5].
21     "</td>");
```

HTML buffer

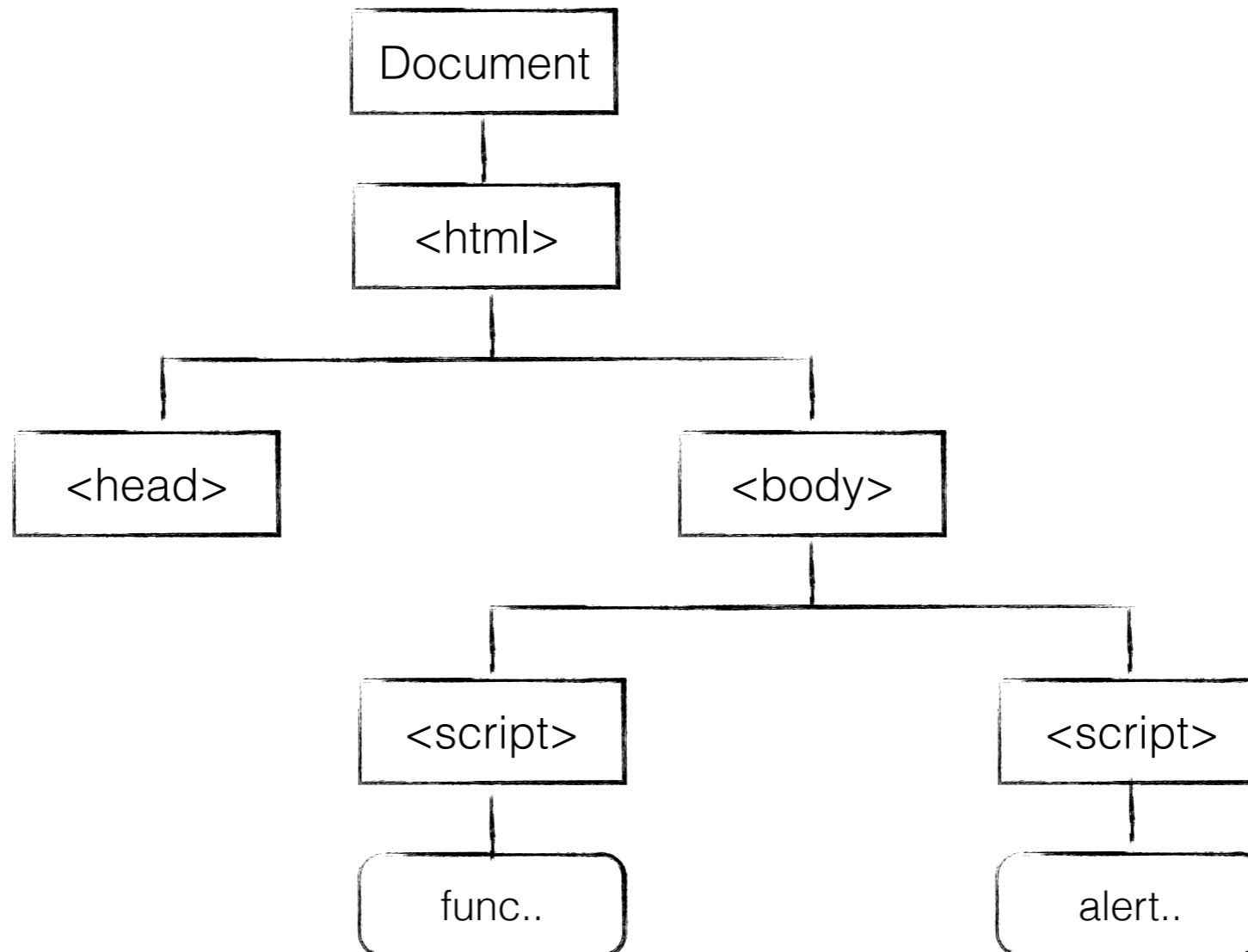
Taint buffer

Source buffer



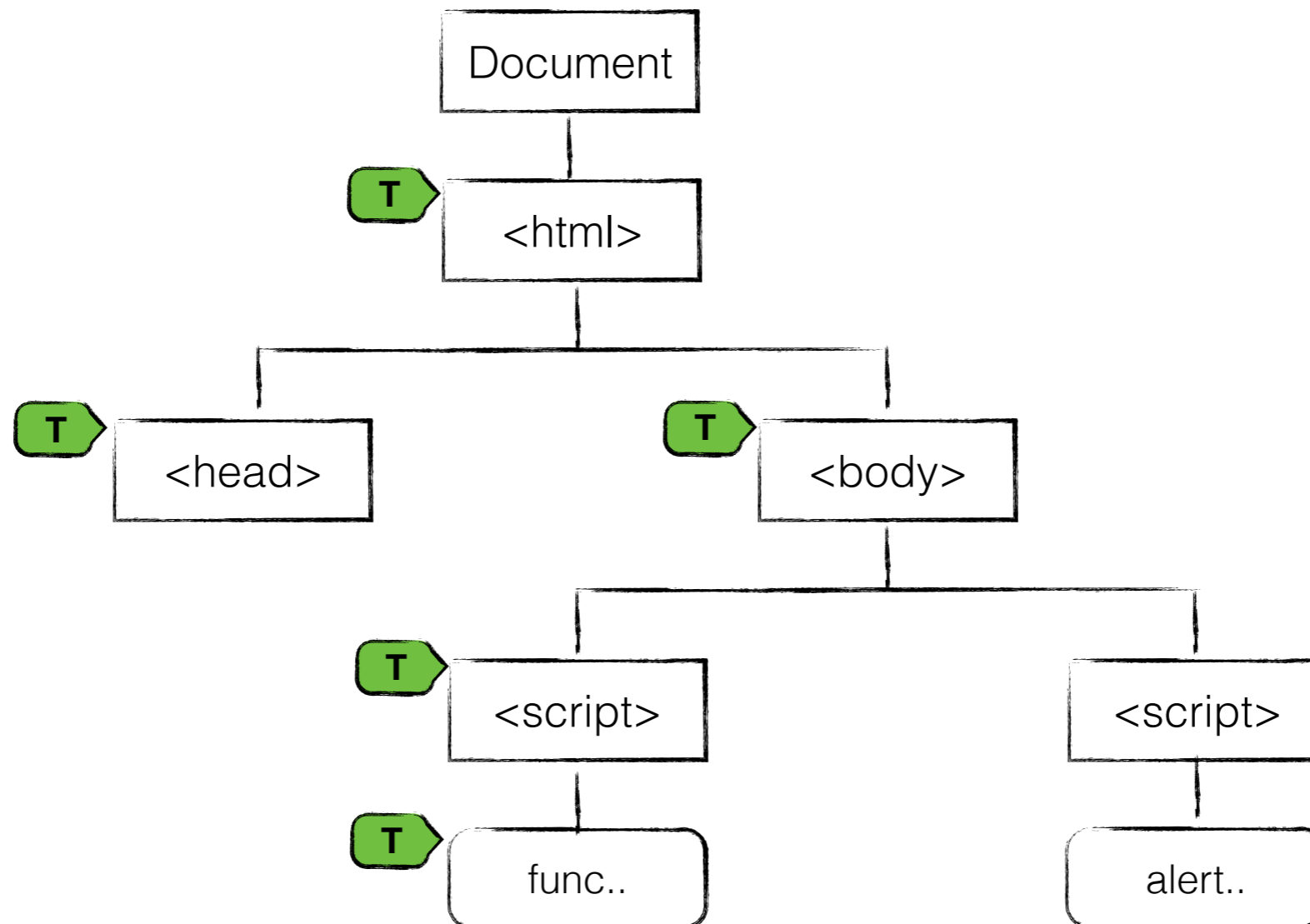
(2) Web Page Analysis

HTML buffer	.	.	<	s	c	r	i	p	t	>	f	u	n	c	.	.	>	.	.	<	s	c	r	i	p	t	>	a	l	e	r	t	.	.		
Taint buffer	.	.	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T
Source buffer	.	.	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	.	.



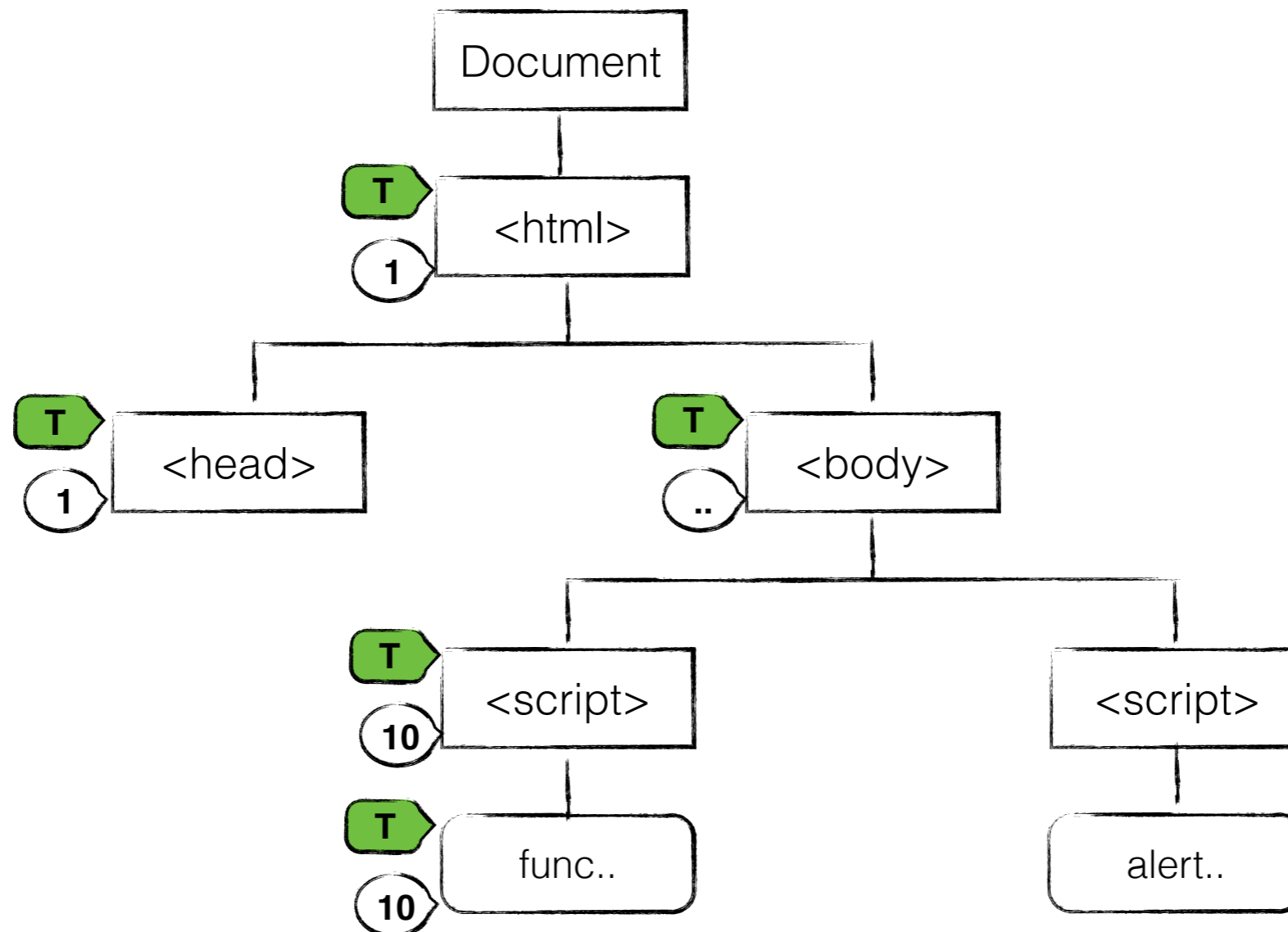
(2) Web Page Analysis

HTML buffer	. . < s c r i p t > f u n c . . > . . < s c r i p t > a l e r t . .
Taint buffer	. . T T T T T T T T T T T T T T T T . .
Source buffer	. . 10 10 10 10 10 10 10 10 10 10 10 10 10 10 . .



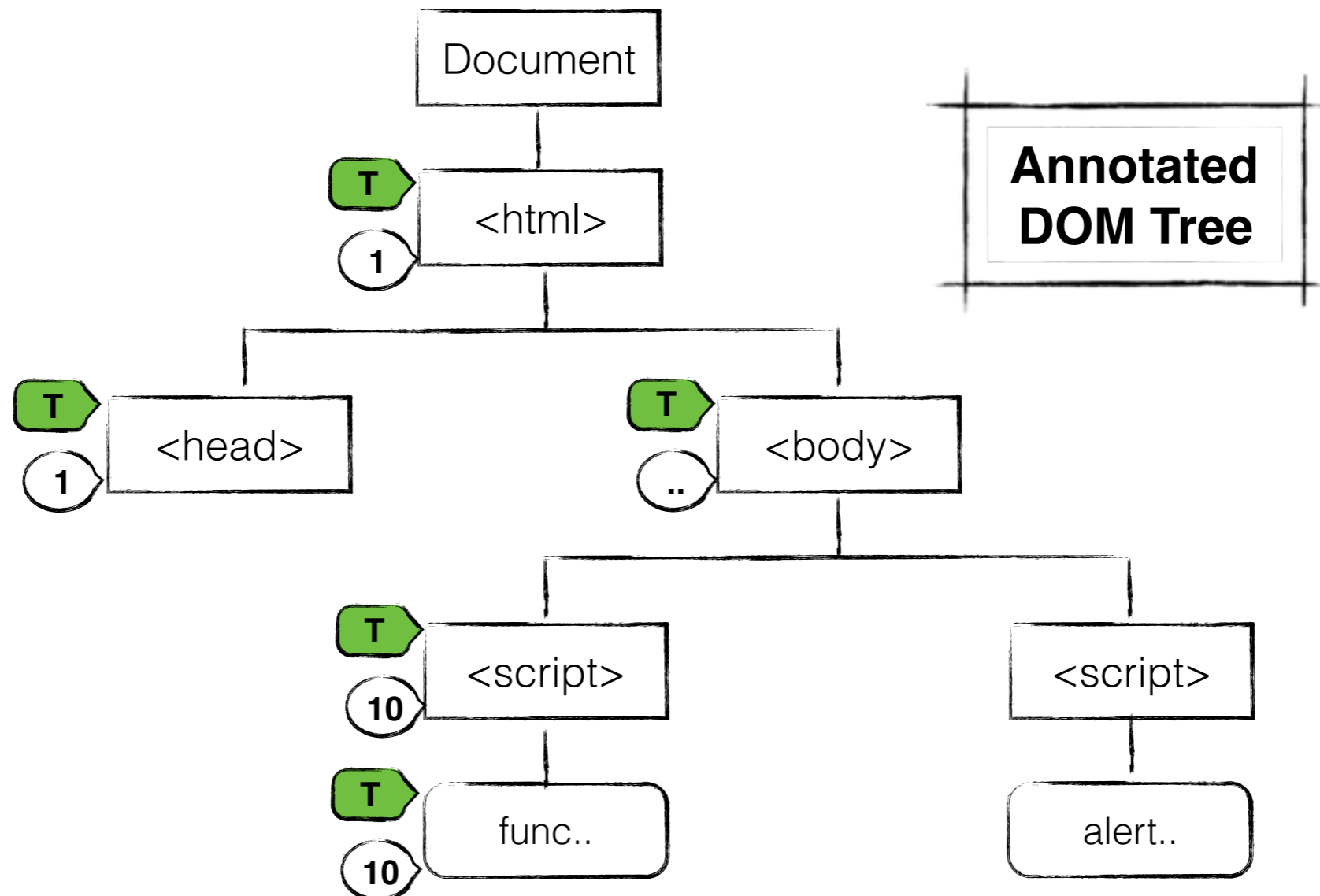
(2) Web Page Analysis

HTML buffer	. . < s c r i p t > f u n c . . > . . < s c r i p t > a l e r t . .
Taint buffer	. . T T T T T T T T T T T T T T T T . .
Source buffer	. . 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 . .

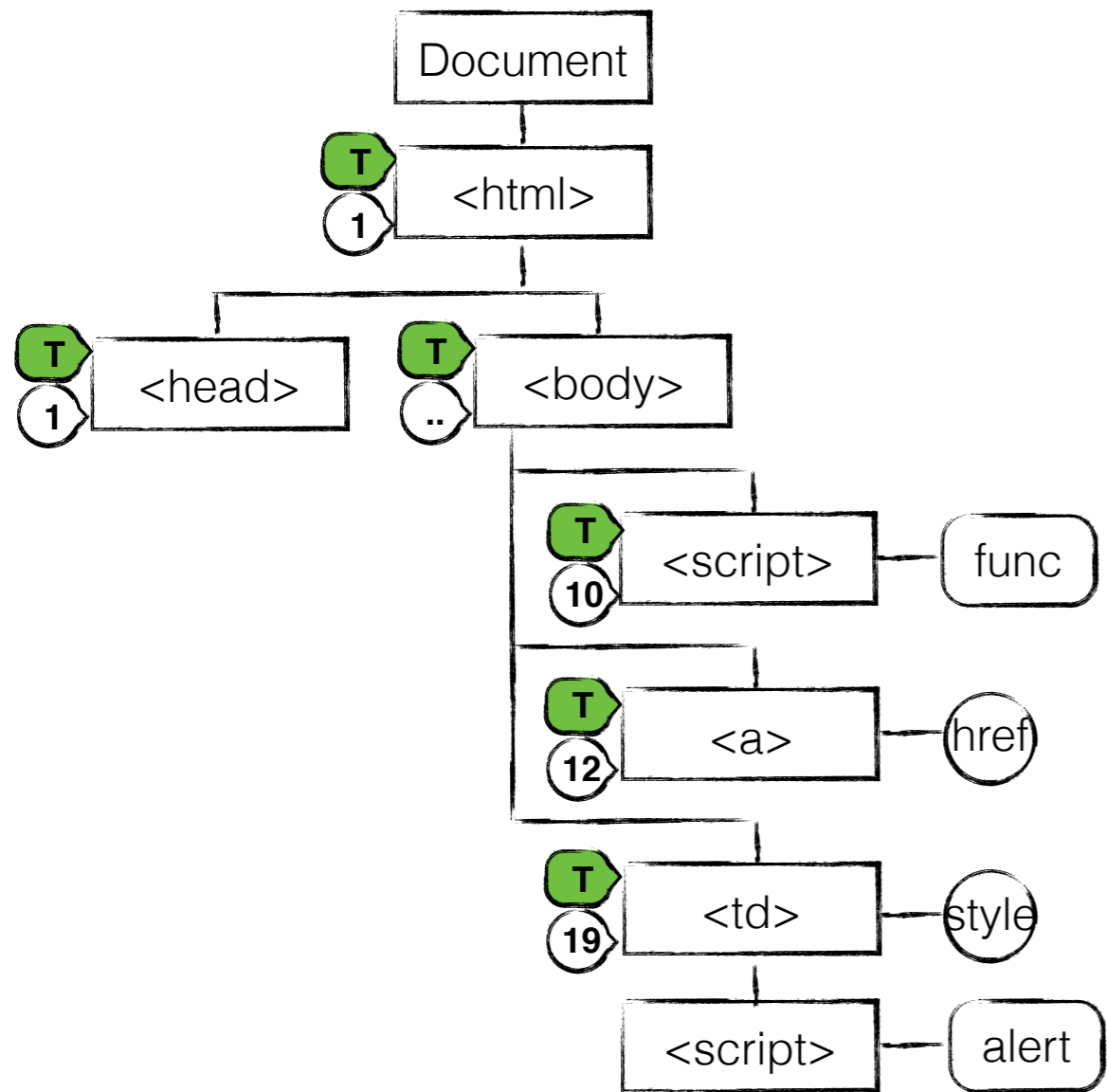


(2) Web Page Analysis

HTML buffer	. . < s c r i p t > f u n c . . > . . < s c r i p t > a l e r t . .
Taint buffer	. . T T T T T T T T T T T T T T T T . .
Source buffer	. . 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 . .

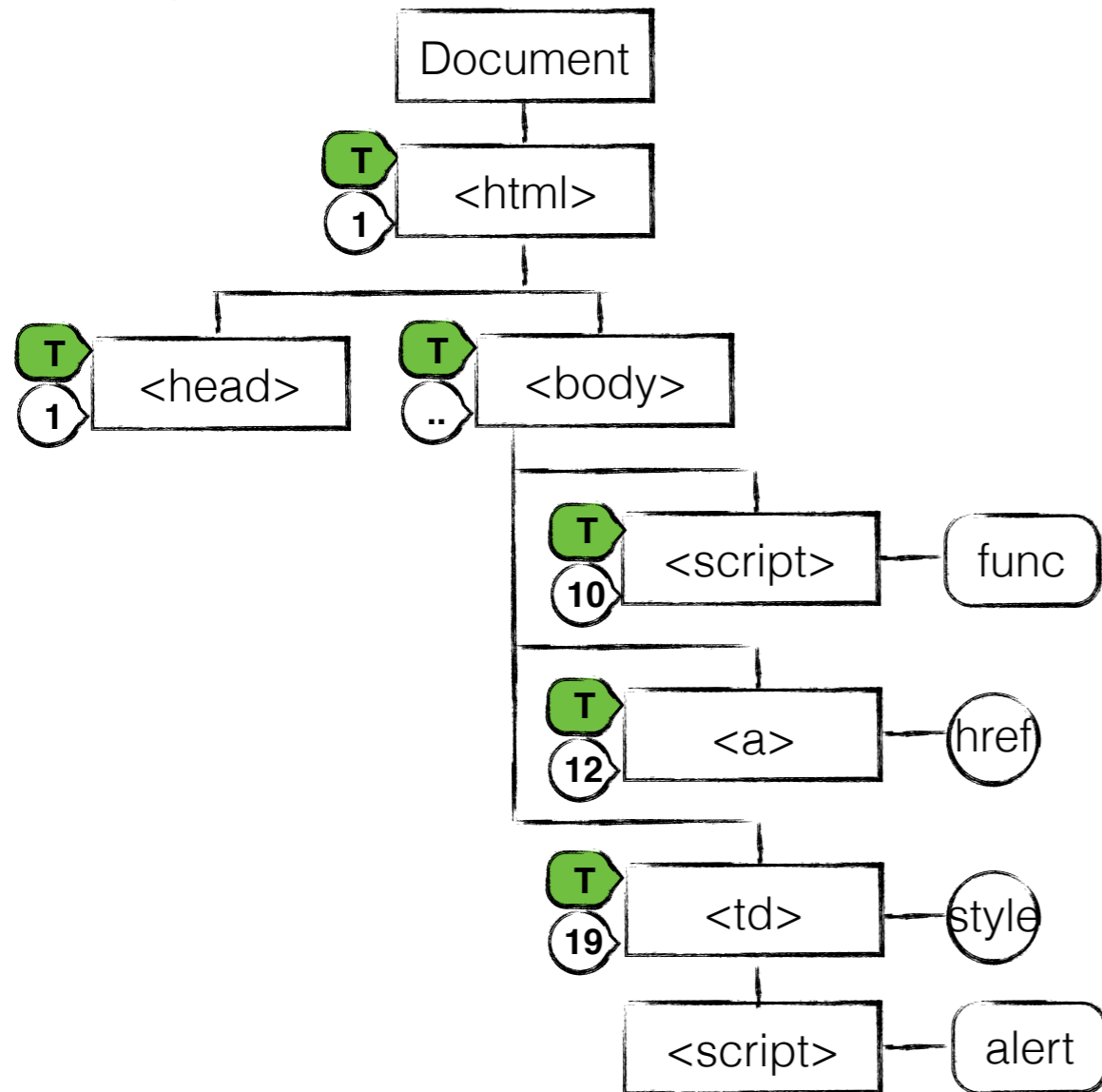


(3) CSP Analysis



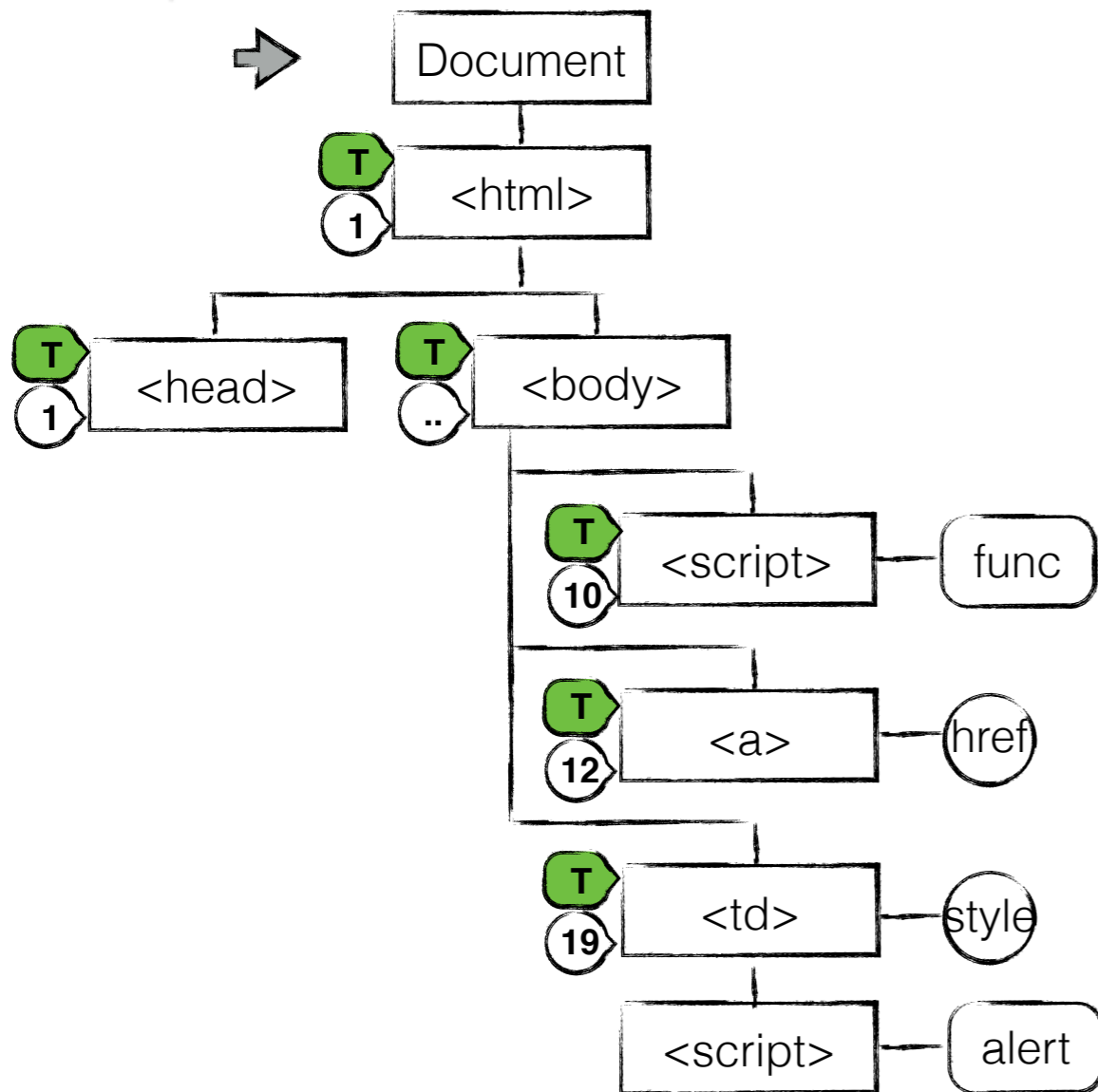
(3) CSP Analysis

Content-Security-Policy: default-src 'none'



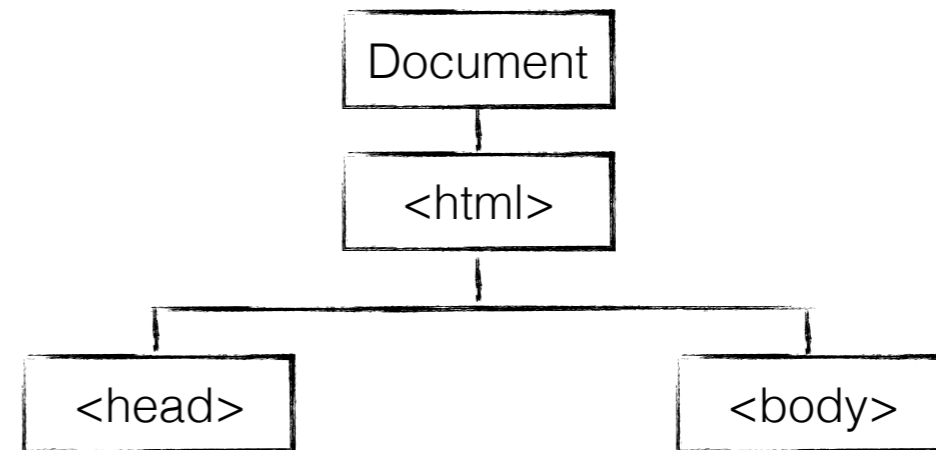
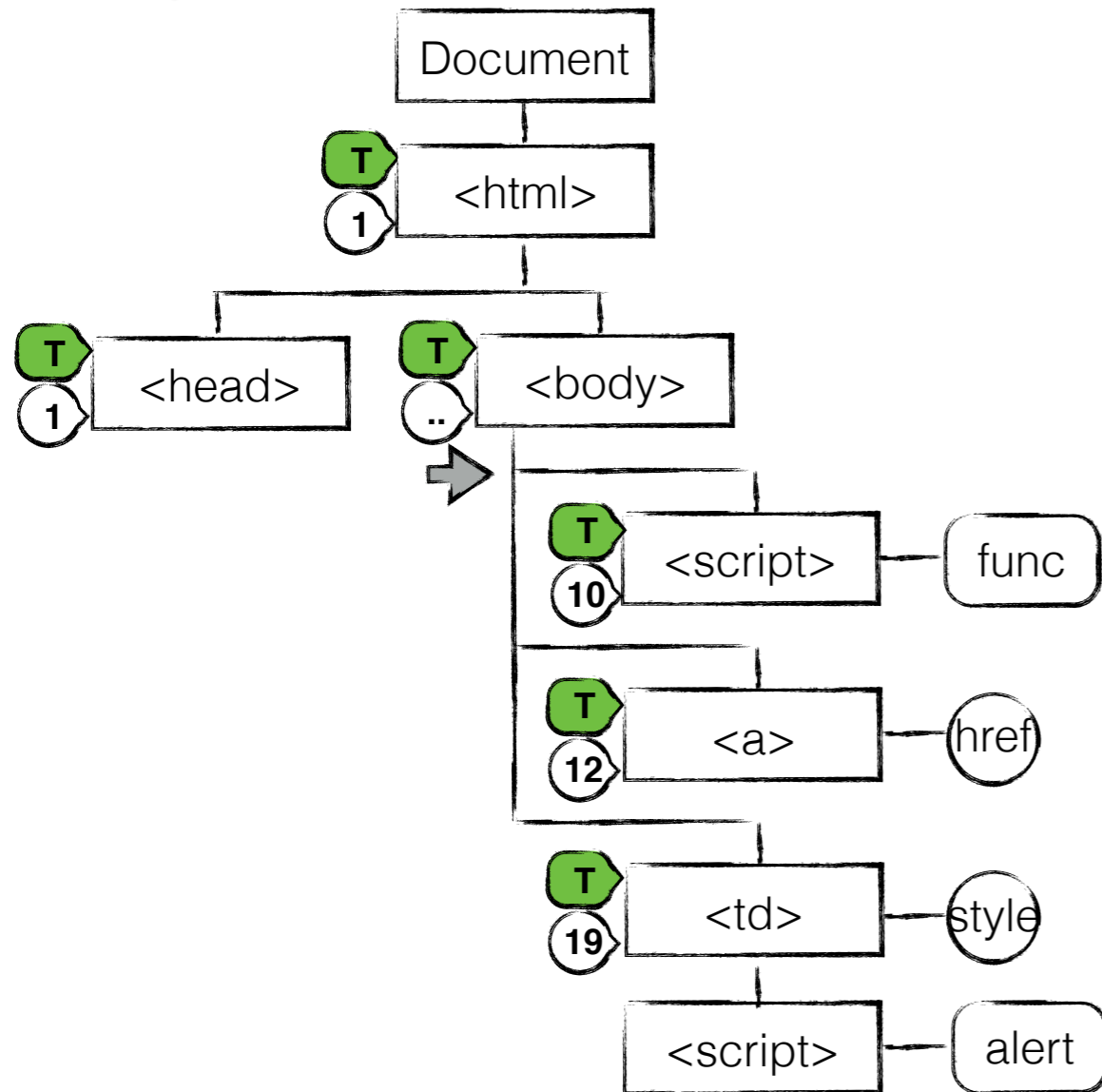
(3) CSP Analysis

Content-Security-Policy: default-src 'none'



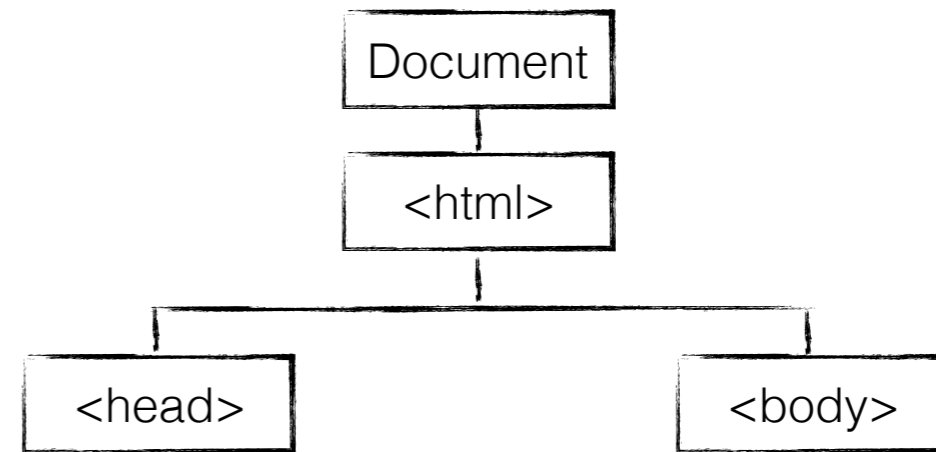
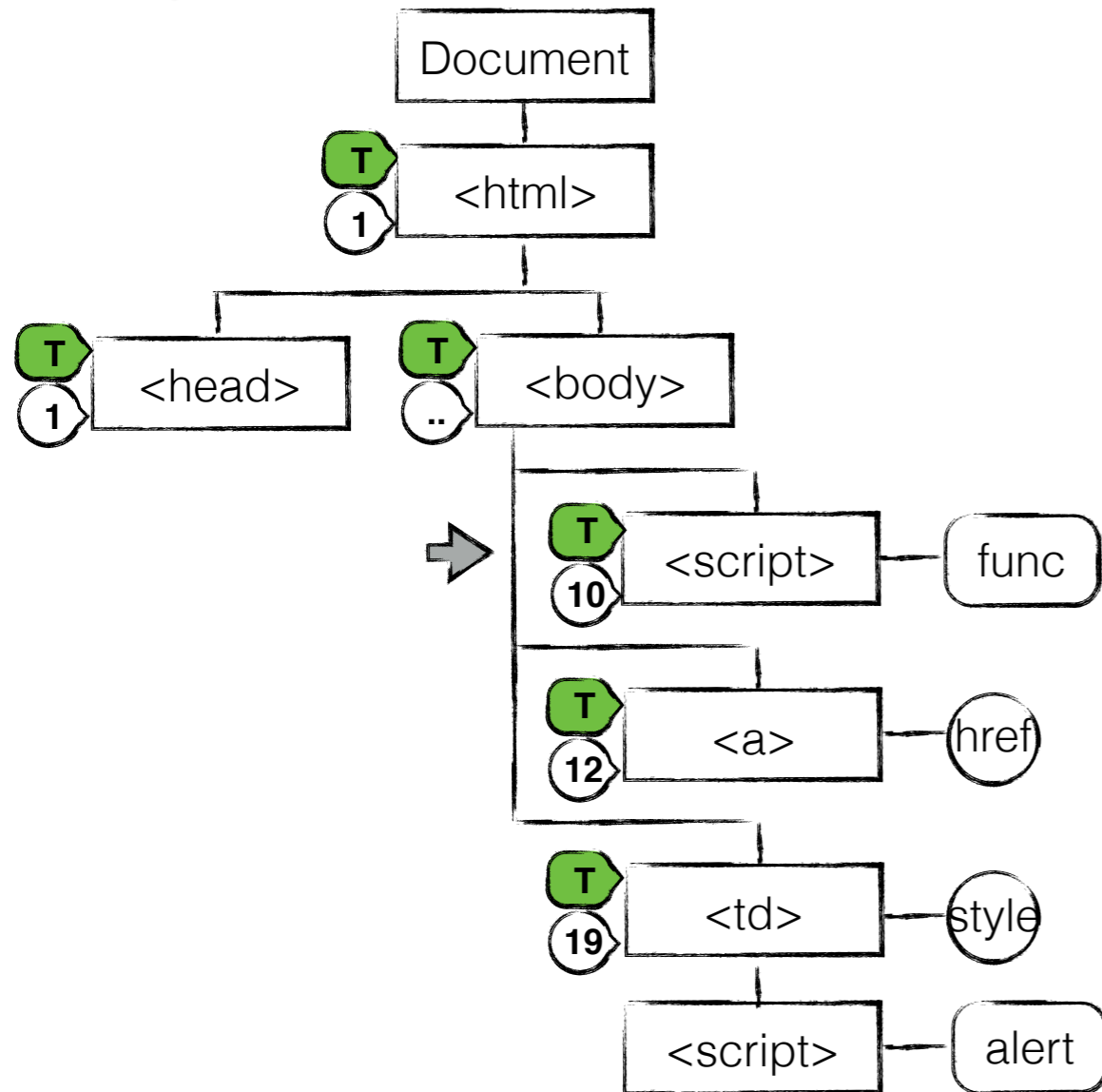
(3) CSP Analysis

Content-Security-Policy: default-src 'none'



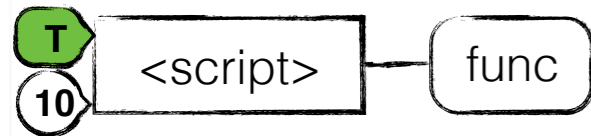
(3) CSP Analysis

Content-Security-Policy: default-src 'none'

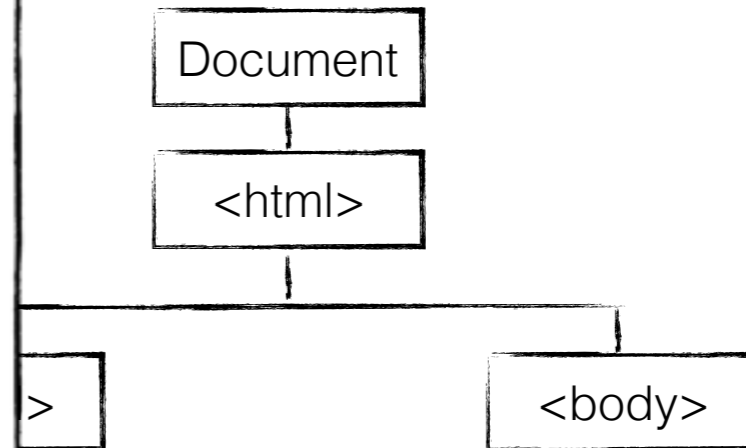


(3) CSP Analysis

Content-Security-Policy: default-src 'none'

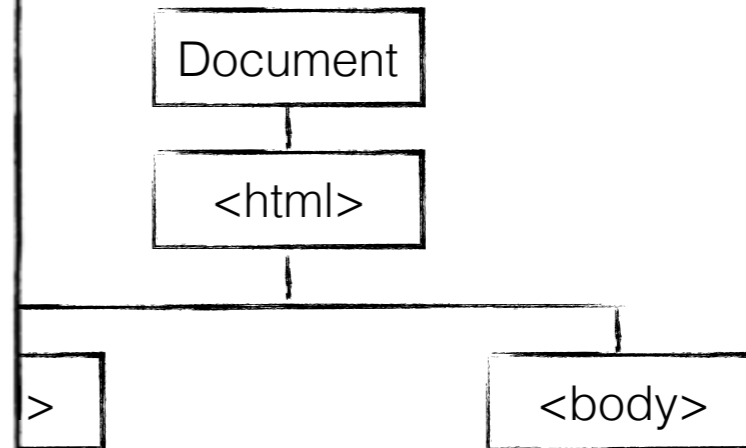
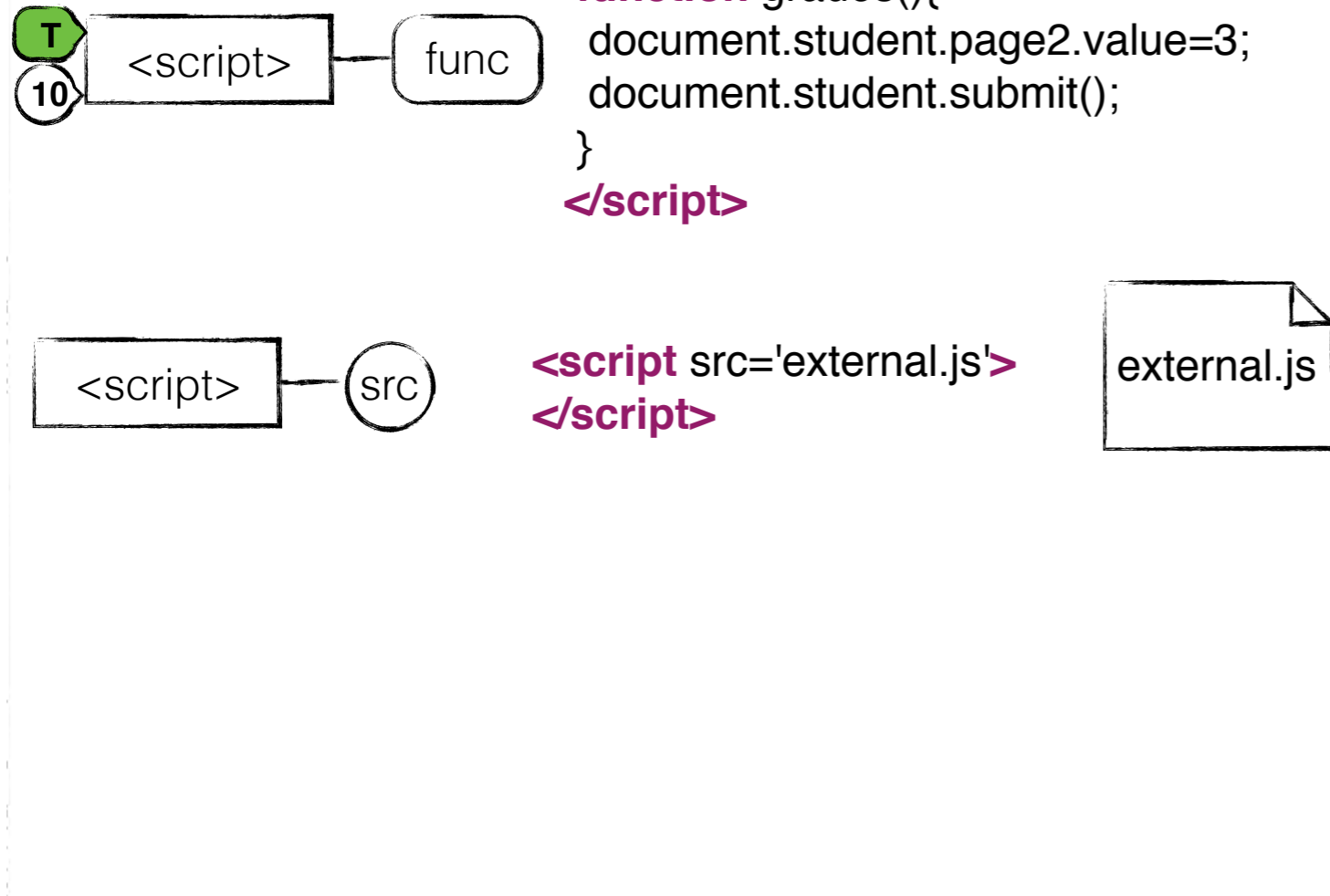


```
<script>  
function grades(){  
  document.student.page2.value=3;  
  document.student.submit();  
}  
</script>
```



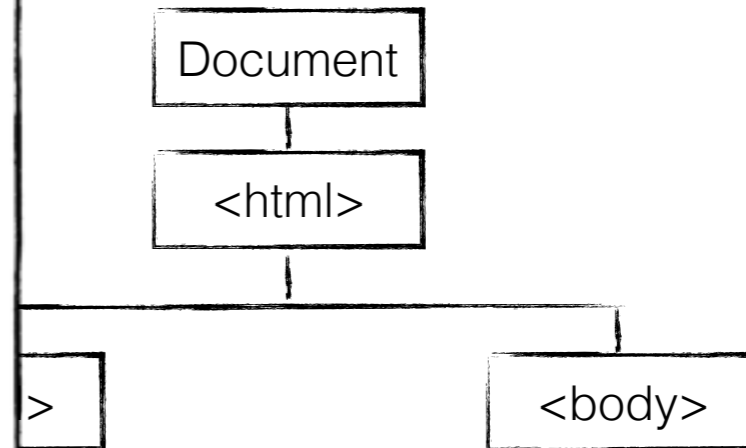
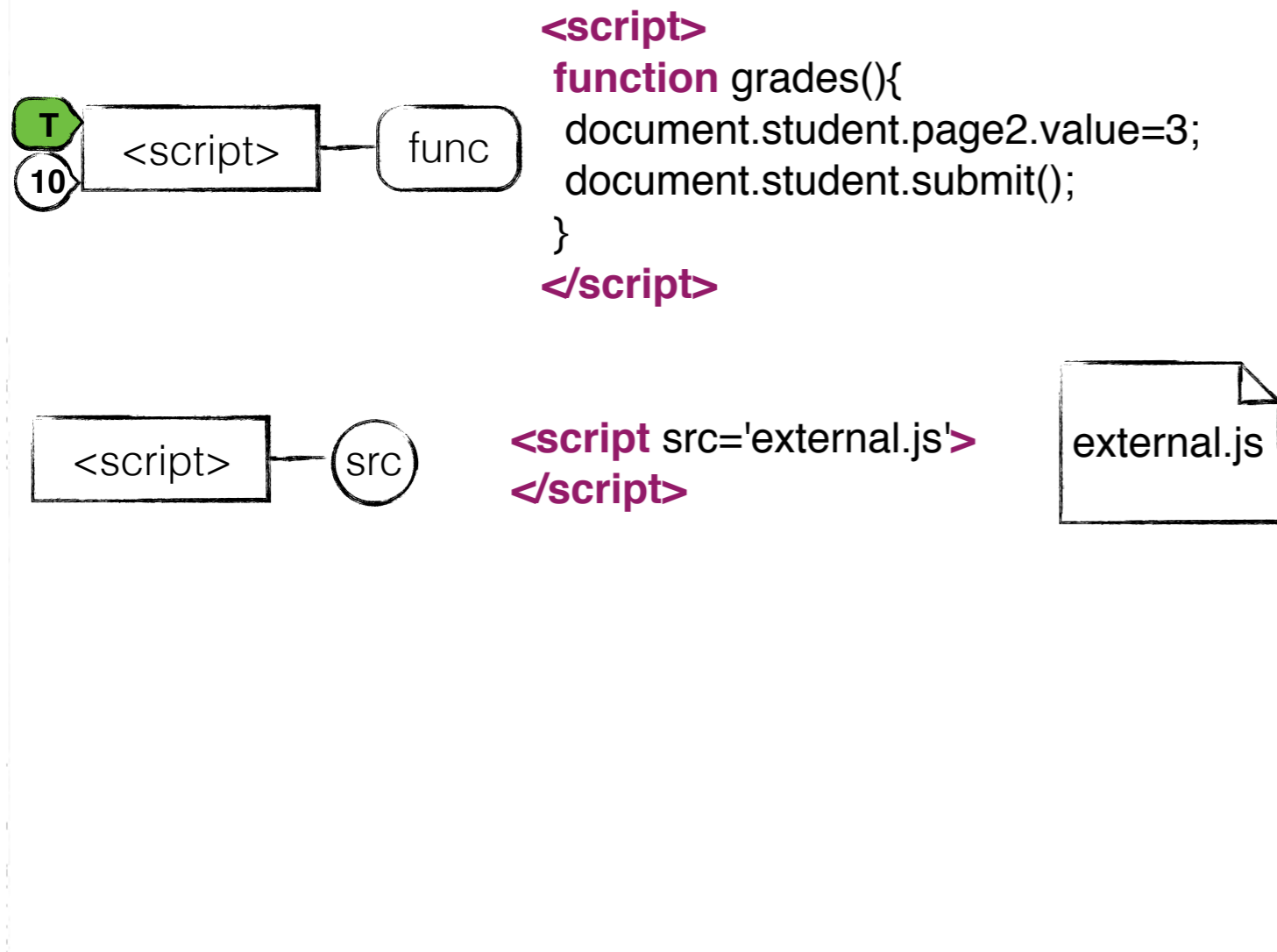
(3) CSP Analysis

Content-Security-Policy: default-src 'none'



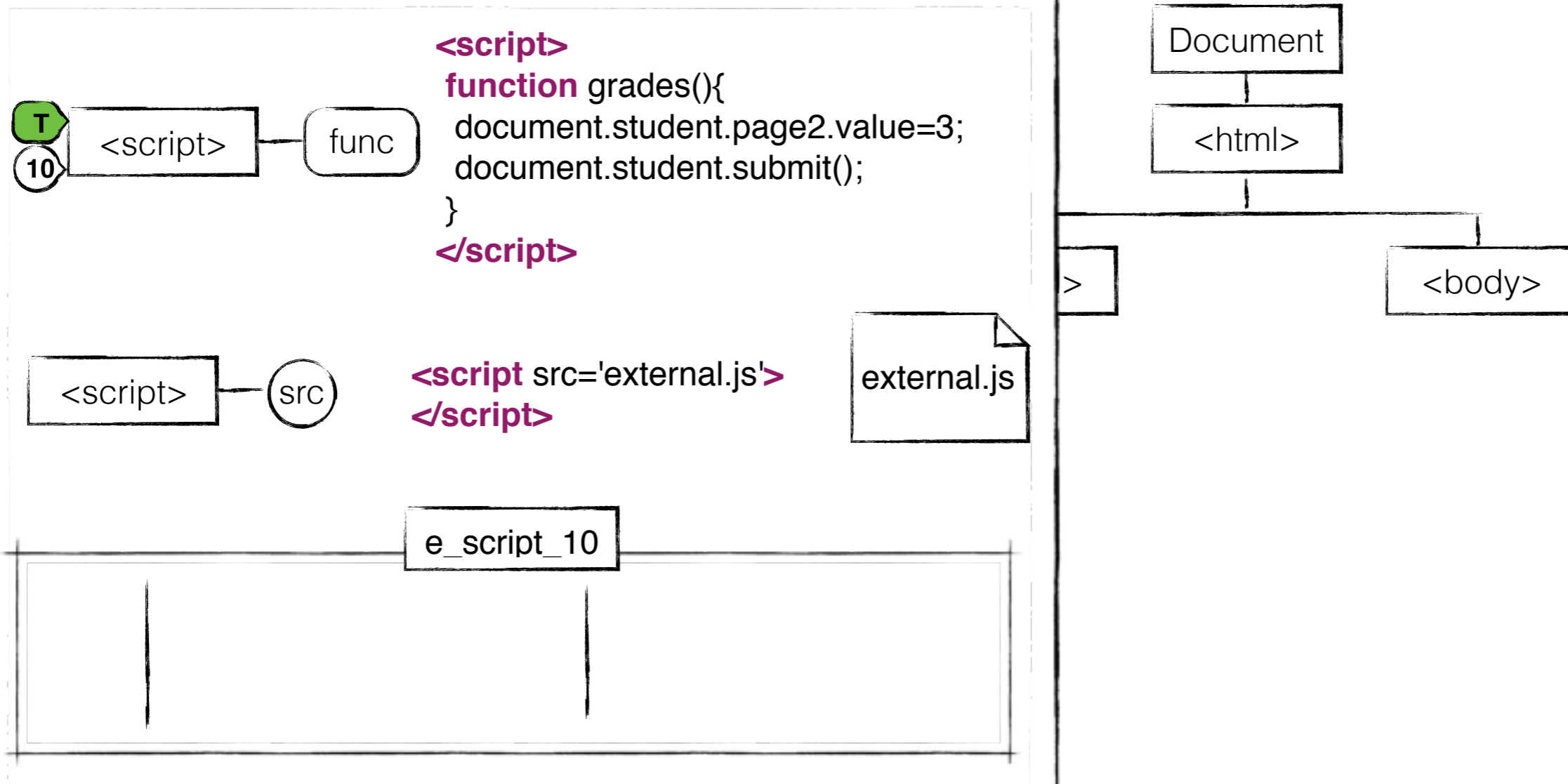
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'



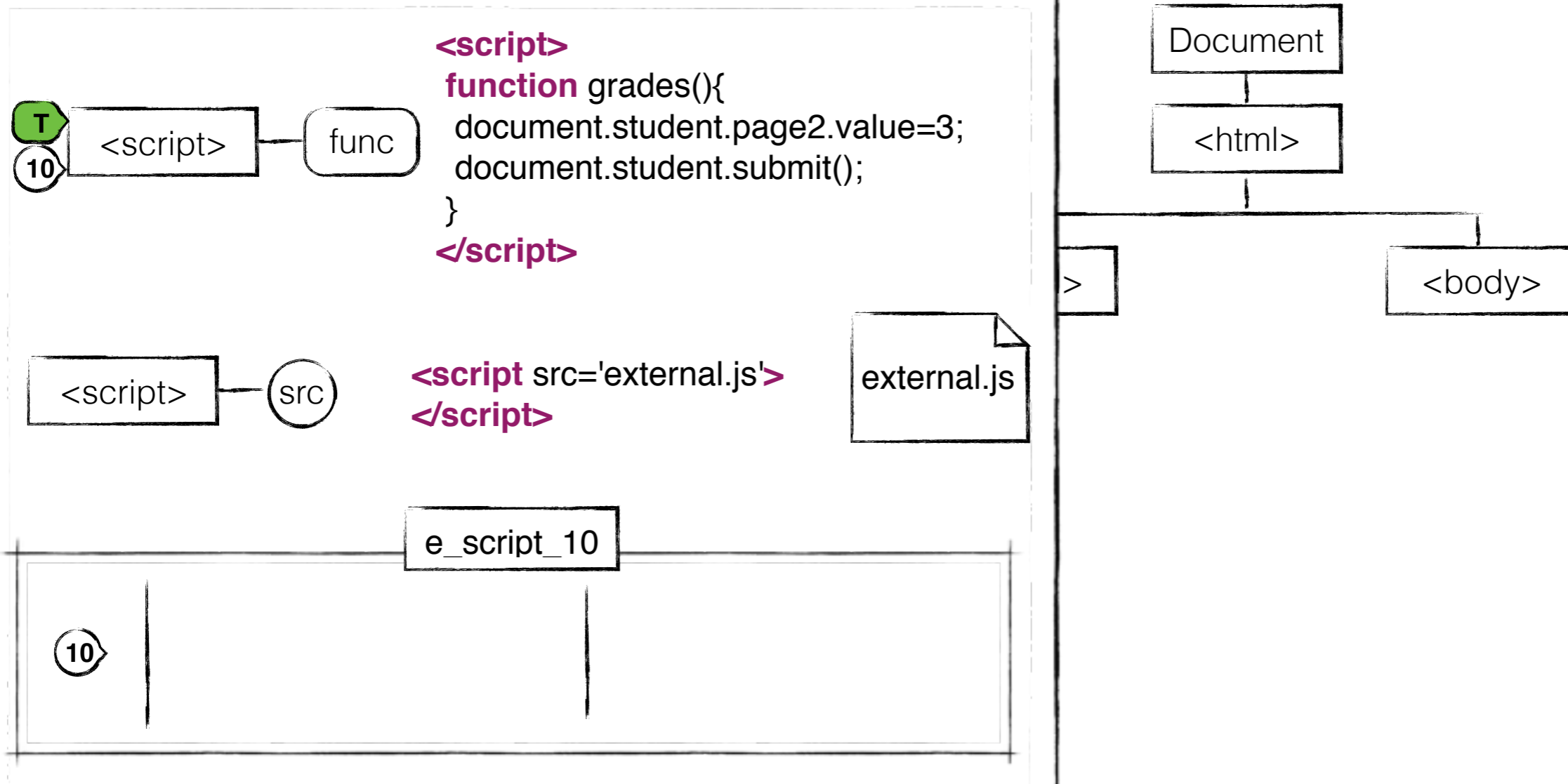
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'



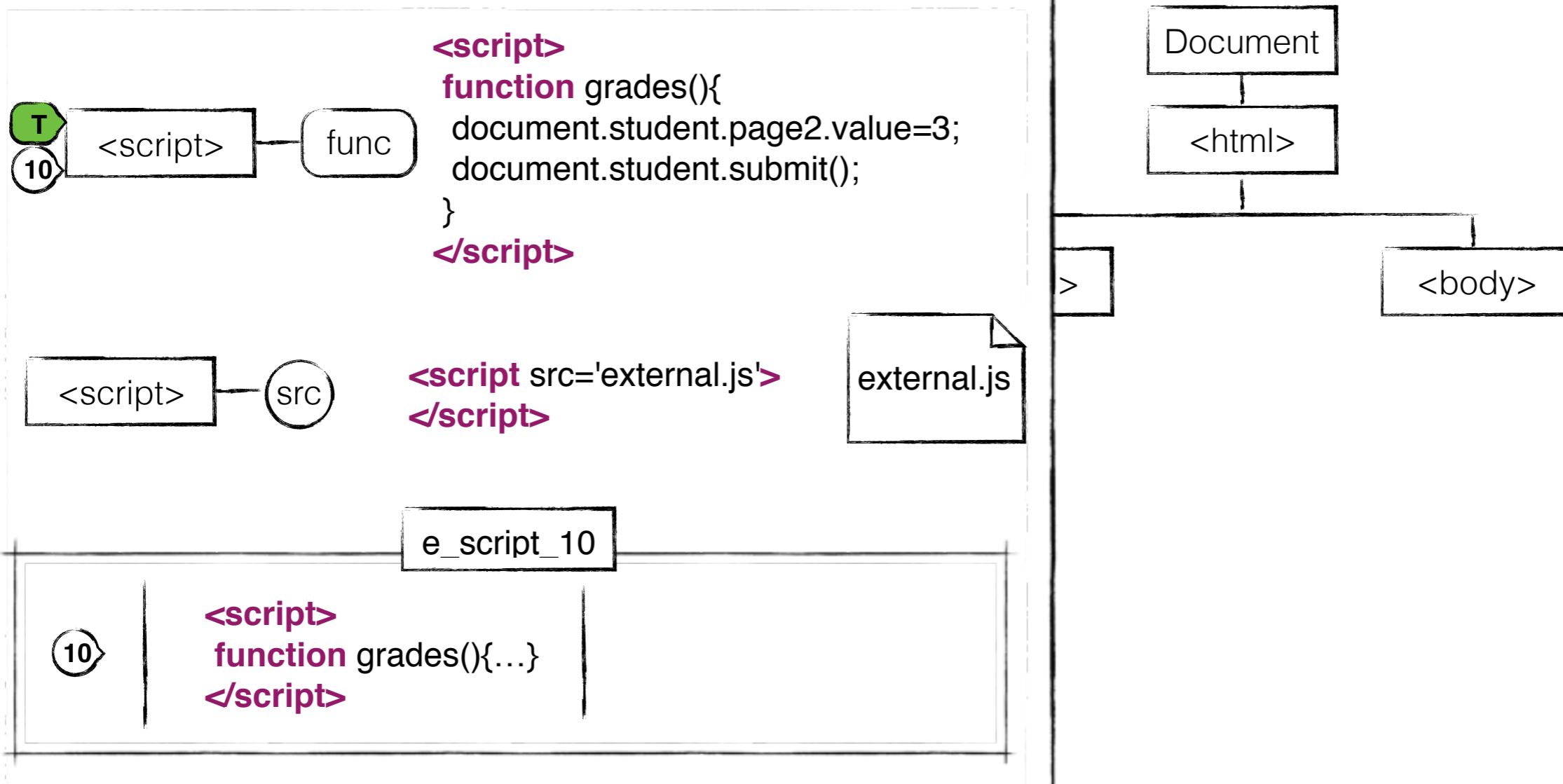
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'



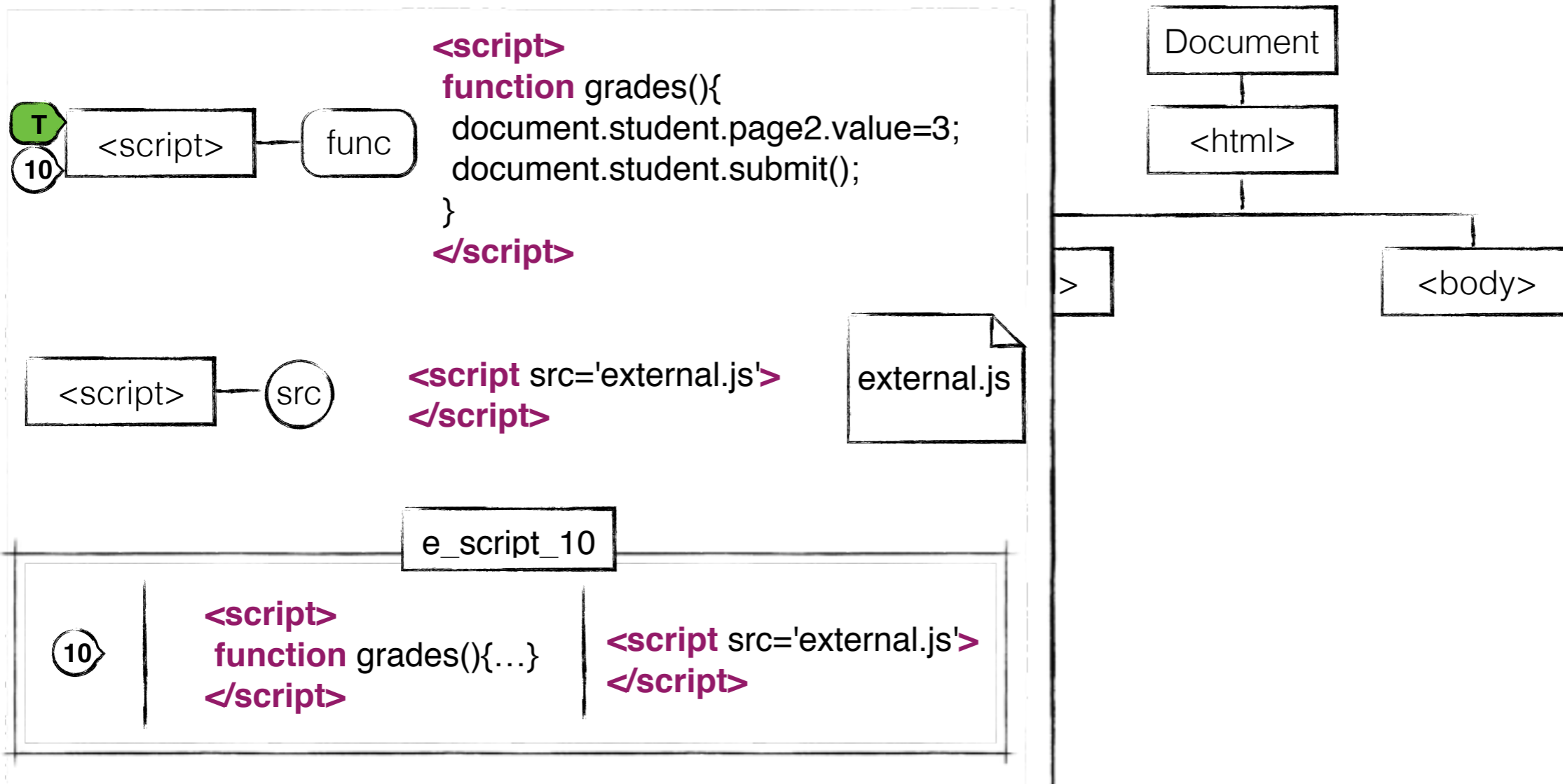
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'



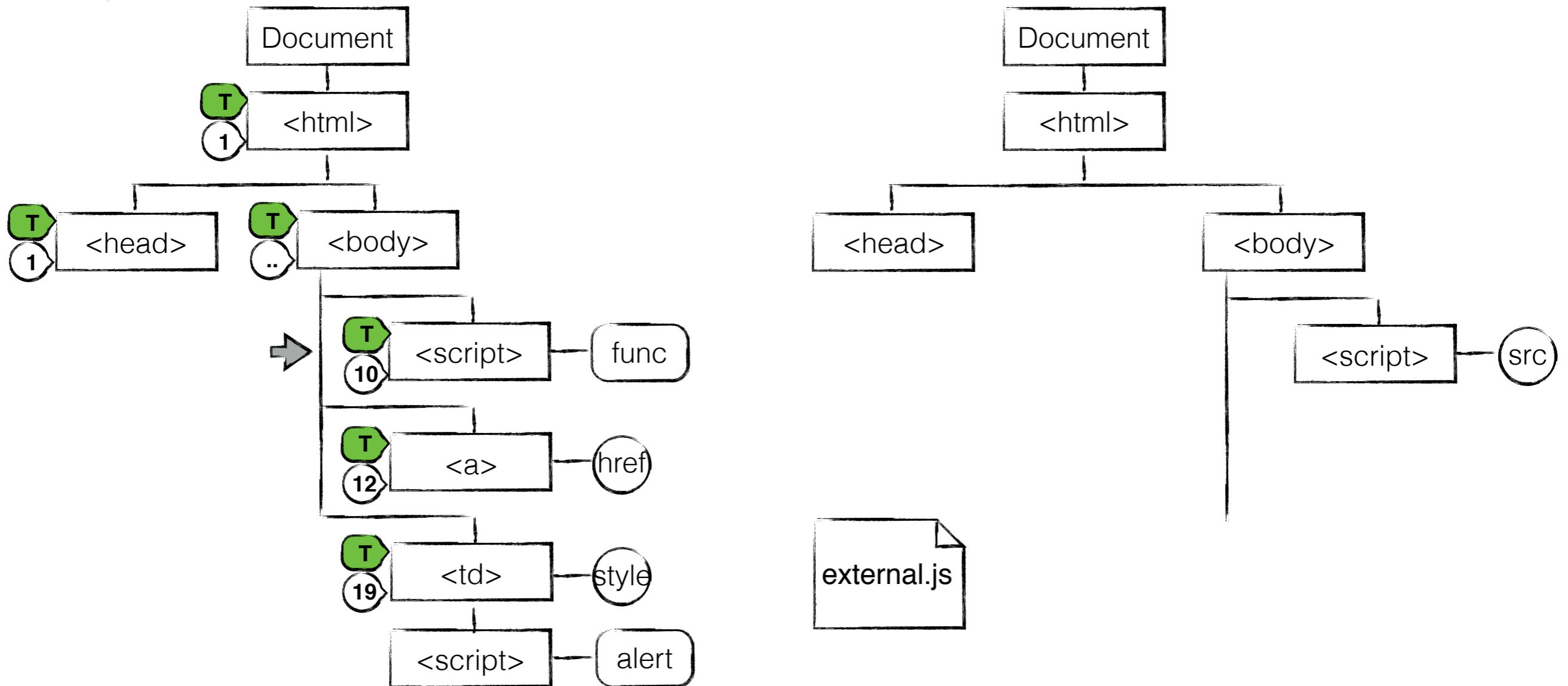
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'



(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'

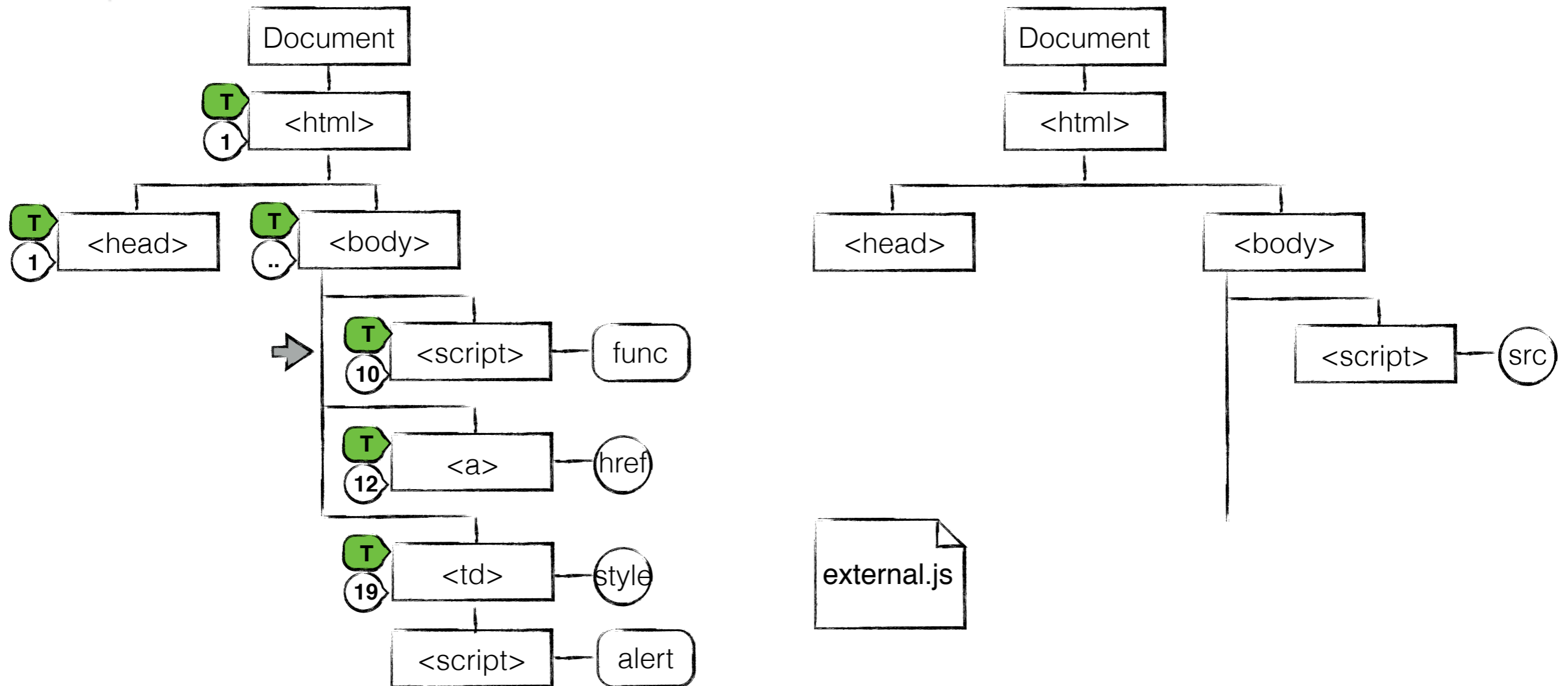


Edit Set

e_script_10

(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'; style-src 'self'

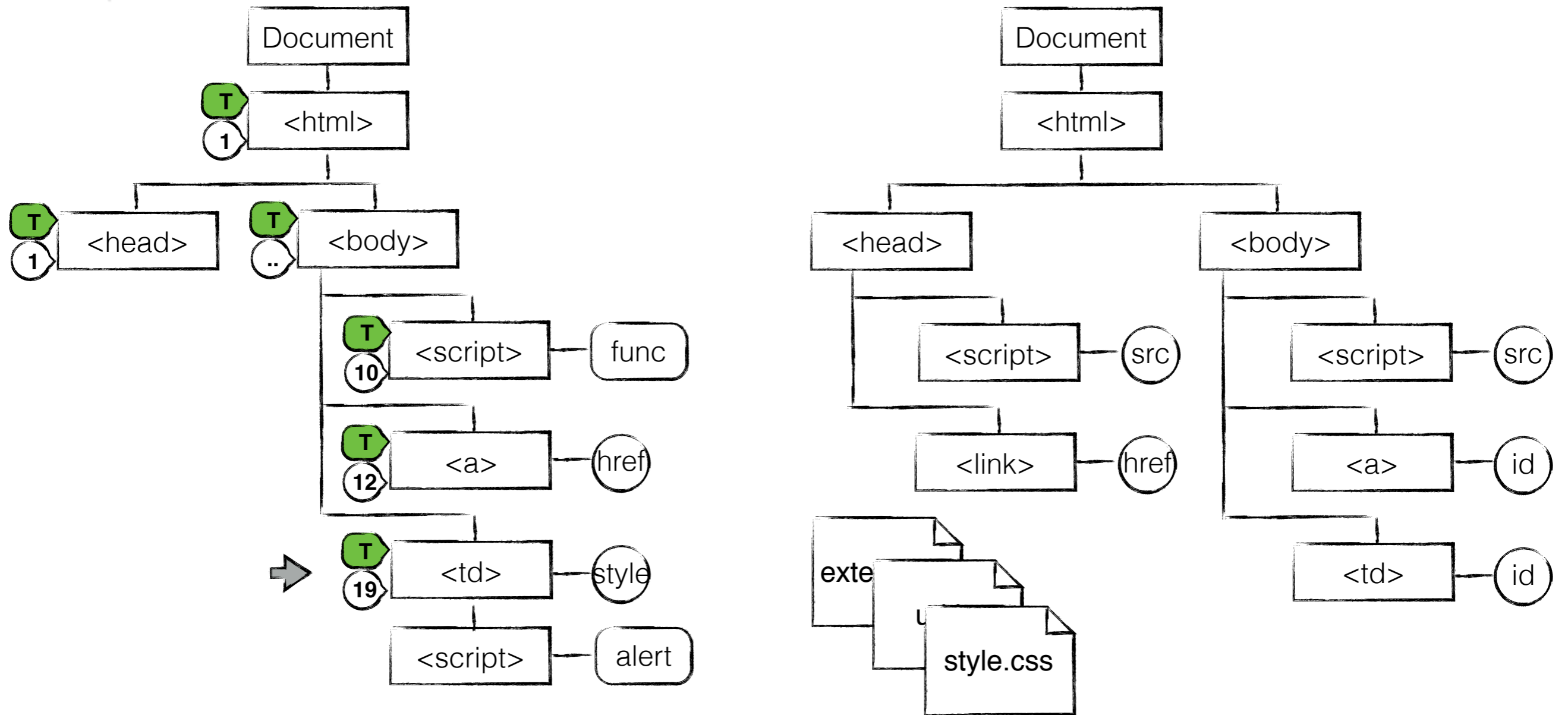


Edit Set

e_script_10

(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'; style-src 'self'



Edit Set

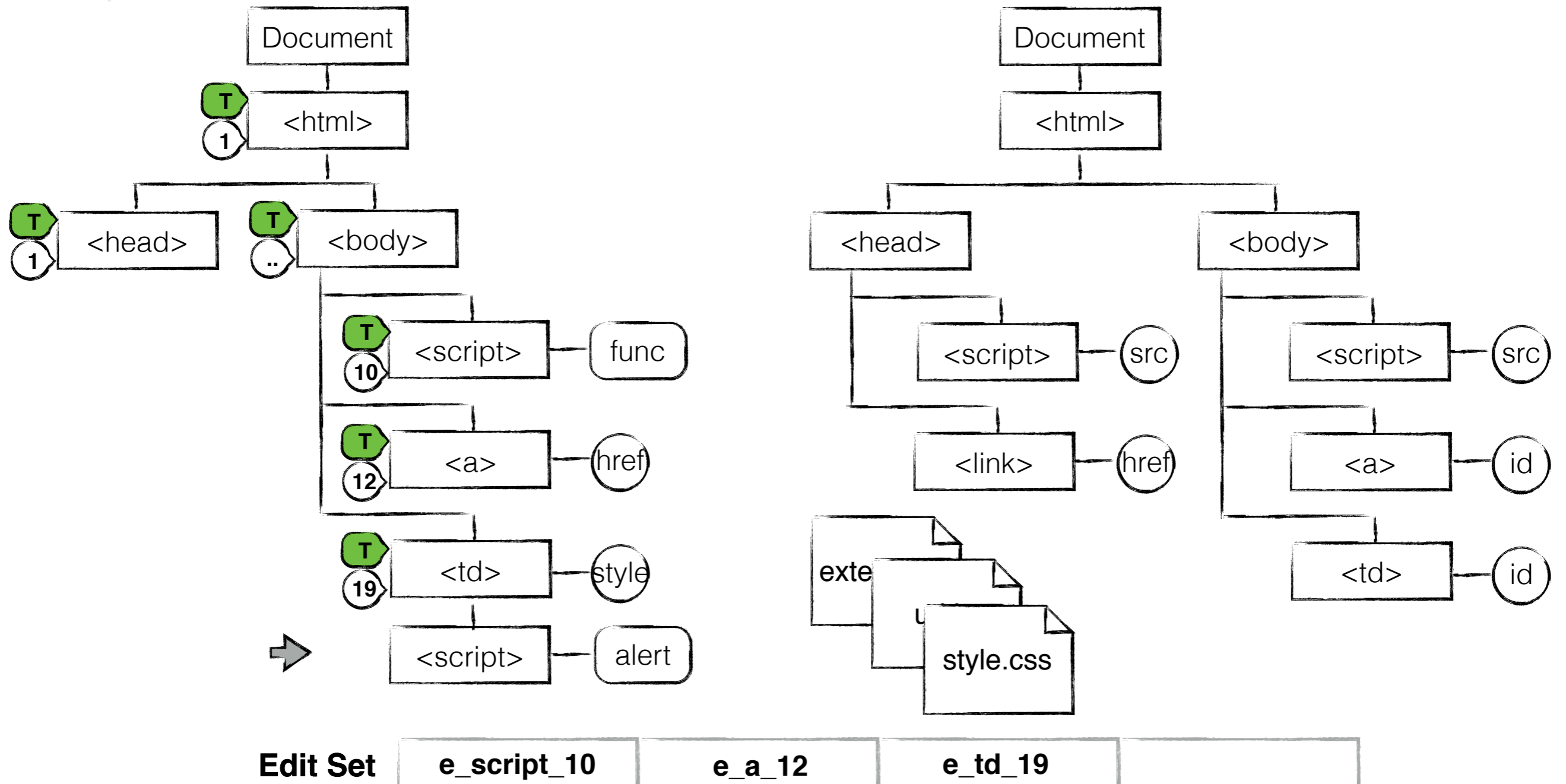
e_script_10

e_a_12

e_td_19

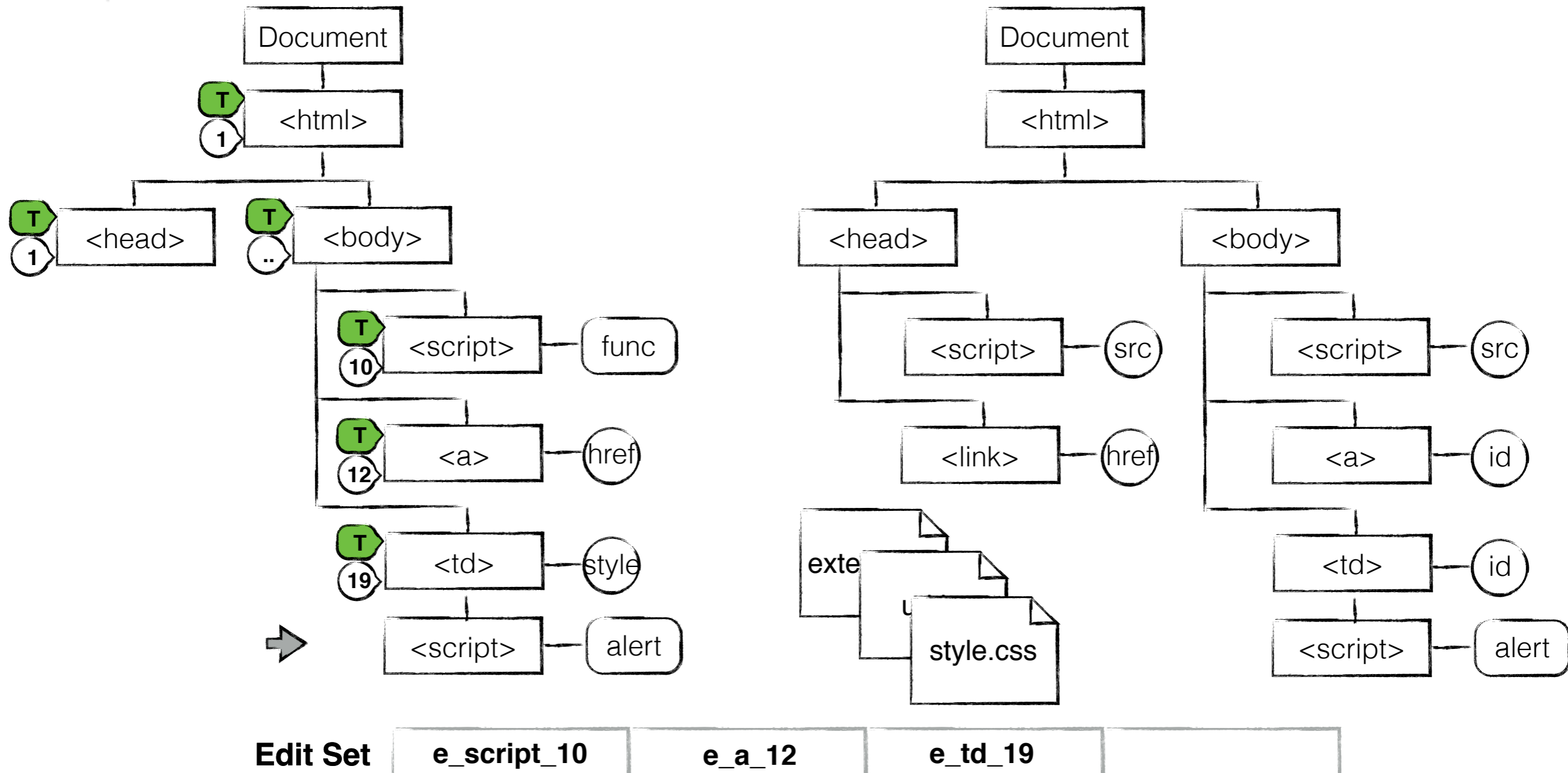
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'; style-src 'self'



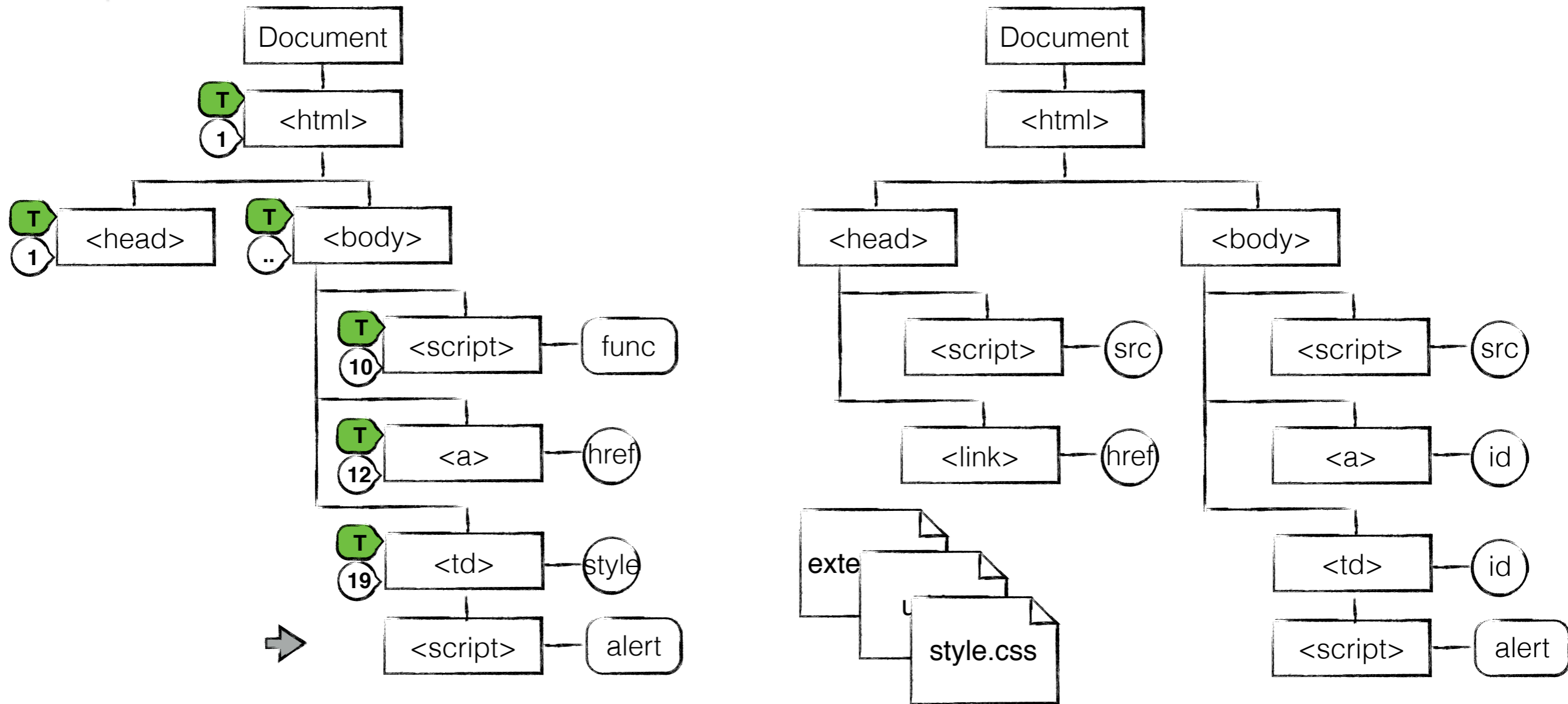
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'; style-src 'self'



(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'; style-src 'self'



Edit Set

e_script_10

e_a_12

e_td_19

e_csp_1

(4) Source Code Transformation

Edit Set

e_script_10

e_a_12

e_td_19

e_csp_1

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

(4) Source Code Transformation



Edit Set

e_script_10

e_a_12

e_td_19

e_csp_1

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

(4) Source Code Transformation



Edit Set

e_script_10

e_a_12

e_td_19

e_csp_1

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

```
function filter_script_10($out){
```

(4) Source Code Transformation



Edit Set

e_script_10

e_a_12

e_td_19

e_csp_1

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

```
function filter_script_10($out){
  $newOut=$out;
  $newScript="<script>function grades(){..}</script>";
  $newScript=str_replace("<script>function grades(){..}</script>",
    "<script src='external.js'></script>",
    $newScript);
}
```

(4) Source Code Transformation



Edit Set

e_script_10

e_a_12

e_td_19

e_csp_1

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades()';>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

```
function filter_script_10($out){
  $newOut=$out;

  $newScript="<script>function grades(){..}</script>";

  $newScript=str_replace("<script>function grades(){..}</script>",
    "<script src='external.js'></script>",
    $newScript);

  $newOut=str_replace("<script>function grades(){..}</script>",
    $newScript,
    $newOut);

  return $newOut;
}
```


(4) Source Code Transformation



Edit Set

e_script_10

e_a_12

e_td_19

e_csp_1

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print(filter_script_10($out));
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

(4) Source Code Transformation



Edit Set

e_script_10

e_a_12

e_td_19

e_csp_1

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

```
1 <?php header("Content-Security-Policy:...");...
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print(filter_script_10($out));
11 ...
12 print(filter_a_12("<a
13 href='javascript:grades();'>
14 Grades</a>"));
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print(filter_td_19"<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>"));
22 ...
23 }
24 print("</html>"); ?>
```

(4) Source Code Transformation

Edit Set

e_script_10

e_a_12

e_td_19

e_csp_1

```
1 <?php print("<html>\n <head>");
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>");
22   ...
23 }
24 print("</html>"); ?>
```

```
1 <?php header("Content-Security-Policy:...");...
2 ...
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print(filter_script_10($out));
11 ...
12 print(filter_a_12("<a
13 href='javascript:grades();'>
14 Grades</a>"));
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18   ...
19   print(filter_td_19"<td style='text-align:left;'>"
20     .$assignment[5].
21     "</td>"));
22   ...
23 }
24 print("</html>"); ?>
```

Implementation

Dynamic Tainting



Web Page Analysis



CSP Analysis



Source Code Transformation



Implementation

Dynamic Tainting



Web Page Analysis



CSP Analysis



Source Code Transformation



Implementation

Dynamic Tainting



Web Page Analysis



CSP Analysis



Source Code Transformation



Implementation

Dynamic Tainting



Web Page Analysis



CSP Analysis



Source Code Transformation



Implementation

Dynamic Tainting



Web Page Analysis



CSP Analysis



Source Code Transformation



Empirical Evaluation

Research Questions:

Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP's performance on the input used for its taint analysis?

Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP's performance on the input used for its taint analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?

Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP's performance on the input used for its taint analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?

Subjects

<i>Benchmark</i>	<i>Type</i>	<i>Version</i>	<i>KLOC</i>
Gallery	Photo Sharing	1.5	34.5
LinPHA	Photo Sharing	1.3	59.6
MyBB	Forum	1.6	105.9
OpenEMR	Medical Management	4.1	480
phpList	Newsletter management	2.10	35.4
Schoolmate	School Management	1.5	6.5
Serendipity	Blogging	0.8	49.6

Subjects

<i>Benchmark</i>	<i>Type</i>	<i>Version</i>	<i>KLOC</i>	<i>MI</i>
Gallery	Photo Sharing	1.5	34.5	4
LinPHA	Photo Sharing	1.3	59.6	4
MyBB	Forum	1.6	105.9	4
OpenEMR	Medical Management	4.1	480	4
phpList	Newsletter management	2.10	35.4	4
Schoolmate	School Management	1.5	6.5	4
Serendipity	Blogging	0.8	49.6	4

Malicious Inputs (MI)

CVE Details



**HTML5 Security
Cheatsheet**

Subjects

<i>Benchmark</i>	<i>Type</i>	<i>Version</i>	<i>KLOC</i>	<i>MI</i>	<i>I</i>
Gallery	Photo Sharing	1.5	34.5	4	16
LinPHA	Photo Sharing	1.3	59.6	4	43
MyBB	Forum	1.6	105.9	4	63
OpenEMR	Medical Management	4.1	480	4	113
phpList	Newsletter management	2.10	35.4	4	77
Schoolmate	School Management	1.5	6.5	4	90
Serendipity	Blogging	0.8	49.6	4	65

Malicious Inputs (MI)

CVE Details



OWASP

**HTML5 Security
Cheatsheet**

Inputs (I)



RQ1(1)

RQ1(1): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ1(1)

RQ1(1): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?



RQ1(1)

RQ1(1): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?



Attacks Blocked

Attacks Blocked

Attacks Blocked

Attacks Blocked



RQ1(2)

RQ1(2): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications' functionality?**

<i>Benchmark</i>	<i>Inputs</i>	<i>None</i>	<i>Self</i>	<i>AutoCSP</i>
Gallery	16	175	68	0
LinPHA	43	231	136	0
MyBB	63	598	364	2
OpenEMR	113	699	533	11
phpList	77	1224	273	1
Schoolmate	90	16	8	0
Serendipity	65	476	385	6

RQ1(2)

RQ1(2): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications' functionality?**

<i>Benchmark</i>	<i>Inputs</i>	<i>None</i>	<i>Self</i>	<i>AutoCSP</i>
Gallery	16	175	68	0
LinPHA	43	231	136	0
MyBB	63	598	364	2
OpenEMR	113	699	533	11
phpList	77	1224	273	1
Schoolmate	90	16	8	0
Serendipity	65	476	385	6

RQ1(2)

RQ1(2): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications' functionality?**

<i>Benchmark</i>	<i>Inputs</i>	<i>None</i>	<i>Self</i>	<i>AutoCSP</i>
Gallery	16	175	68	0
LinPHA	43	231	136	0
MyBB	63	598	364	2
OpenEMR	113	699	533	11
phpList	77	1224	273	1
Schoolmate	90	16	8	0
Serendipity	65	476	385	6

RQ1(2)

RQ1(2): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications' functionality?**

<i>Benchmark</i>	<i>Inputs</i>	<i>None</i>	<i>Self</i>	<i>AutoCSP</i>
Gallery	16	175	68	0
LinPHA	43	231	136	0
MyBB	63	598	364	2
OpenEMR	113	699	533	11
phpList	77	1224	273	1
Schoolmate	90	16	8	0
Serendipity	65	476	385	6

RQ1(2)

RQ1(2): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications' functionality?**

<i>Benchmark</i>	<i>Inputs</i>	<i>None</i>	<i>Self</i>	<i>AutoCSP</i>
Gallery	16	175	68	0
LinPHA	43	231	136	0
MyBB	63	598	364	2
OpenEMR	113	699	533	11
phpList	77	1224	273	1
Schoolmate	90	16	8	0
Serendipity	65	476	385	6

RQ1(2)

RQ1(2): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications' functionality?**

<i>Benchmark</i>	<i>Inputs</i>	<i>None</i>	<i>Self</i>	<i>AutoCSP</i>
Gallery	16	175	68	0
LinPHA	43	231	136	0
MyBB	63	598	364	2
OpenEMR	113	699	533	11
phpList	77	1224	273	1
Schoolmate	90	16	8	0
Serendipity	65	476	385	6

RQ1(2)

RQ1(2): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications' functionality?**

<i>Benchmark</i>	<i>Inputs</i>	<i>None</i>	<i>Self</i>	<i>AutoCSP</i>
Gallery	16	175	68	0
LinPHA	43	231	136	0
MyBB	63	598	364	2
OpenEMR	113	699	533	11
phpList	77	1224	273	1
Schoolmate	90	16	8	0
Serendipity	65	476	385	6

E1: client-side execution of eval.

```
var x = eval('...');
```

E2: client-side creation on inline script nodes.

```
document.write('<script>...</script>');
```

E3: client-side creation on inline style nodes.

```
document.write('<style>...</style>');
```

RQ4

RQ4: Is automation actually needed to retrofit CSP to web applications?

<i>Benchmark</i>	E_{csp}	E_e	F
Gallery	2	76	12
LinPHA	2	67	11
MyBB	5	97	6
OpenEMR	31	319	52
phpList	1	33	8
Schoolmate	1	328	26
Serendipity	5	103	16

RQ4

RQ4: Is automation actually needed to retrofit CSP to web applications?

<i>Benchmark</i>	E_{csp}	E_e	F
Gallery	2	76	12
LinPHA	2	67	11
MyBB	5	97	6
OpenEMR	31	319	52
phpList	1	33	8
Schoolmate	1	328	26
Serendipity	5	103	16

E_{csp} : number of CSP edits.

RQ4

RQ4: Is automation actually needed to retrofit CSP to web applications?

<i>Benchmark</i>	E_{csp}	E_e	F
Gallery	2	76	12
LinPHA	2	67	11
MyBB	5	97	6
OpenEMR	31	319	52
phpList	1	33	8
Schoolmate	1	328	26
Serendipity	5	103	16

E_{csp} : number of CSP edits.

E_e : number of modified HTML elements.

RQ4

RQ4: Is automation actually needed to retrofit CSP to web applications?

<i>Benchmark</i>	E_{csp}	E_e	F
Gallery	2	76	12
LinPHA	2	67	11
MyBB	5	97	6
OpenEMR	31	319	52
phpList	1	33	8
Schoolmate	1	328	26
Serendipity	5	103	16

E_{csp} : number of CSP edits.

E_e : number of modified HTML elements.

E_{csp} : number of modified files.

Evaluation Summary

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

AutoCSP offers effective protection against XSS.

AutoCSP introduces low number of false alarms.

RQ4: Is automation actually needed to retrofit CSP to web applications?

Automation is needed.

Related Work

Content Security Policy

Doupé et al., Stamm et al., and Weinberger et al.

Web Page Security Policies

Jim et al. and Louw et al.

Dynamic Tainting in Web Applications Security

Halfond et al., Nguyen-Tuong, and Pietraszek et al.

Related Work

Content Security Policy

Doupé et al., Stamm et al., and Weinberger et al.

Web Page Security Policies

Jim et al. and Louw et al.

Dynamic Tainting in Web Applications Security

Halfond et al., Nguyen-Tuong, and Pietraszek et al.

Related Work

Content Security Policy

Doupé et al., Stamm et al., and Weinberger et al.

Web Page Security Policies

Jim et al. and Louw et al.

Dynamic Tainting in Web Applications Security

Halfond et al., Nguyen-Tuong, and Pietraszek et al.

Related Work

Content Security Policy

Doupé et al., Stamm et al., and Weinberger et al.

Web Page Security Policies

Jim et al. and Louw et al.

Dynamic Tainting in Web Applications Security

Halfond et al., Nguyen-Tuong, and Pietraszek et al.

Summary

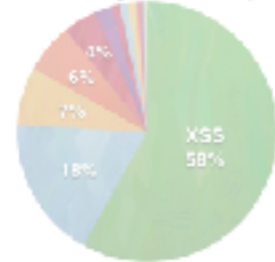
Cross-Site Scripting (XSS)



- 18 Sep 2014: "eBay Under Fire After Cross Site Scripting Attack"
- 16 Sep 2013: "NASDAQ Website Vulnerable to XSS Attacks"
- 26 May 2013: "PayPal vulnerable to cross-site scripting again"



Vulnerability Classes (2014)



Wired for Security, 2014

Content Security Policy (CSP)

Server CSP Client

11 37 42 8 27

AutoCSP



Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP's performance on the input used for its taint analysis?

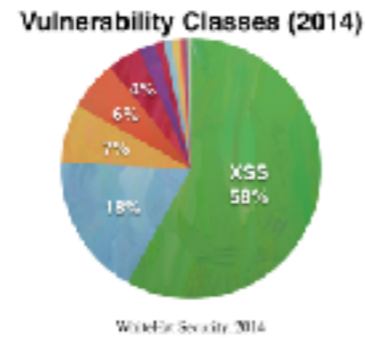
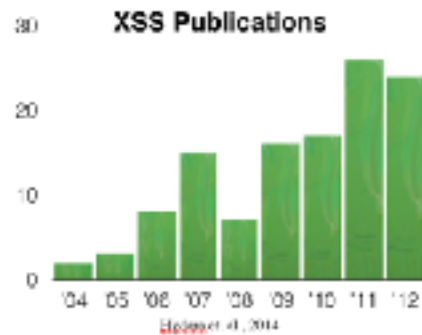
RQ4: Is automation actually needed to retrofit CSP to web applications?

Summary

Cross-Site Scripting (XSS)



- 18 Sep 2014 "eBay Under Fire After Cross Site Scripting Attack"
- 16 Sep 2013 "NASDAQ Website Vulnerable to XSS Attacks"
- 26 May 2013 "PayPal vulnerable to cross-site scripting again"



Content Security Policy (CSP)

Server CSP Client

11 37 42 8 27

AutoCSP



Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP's performance on the input used for its taint analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?

Summary

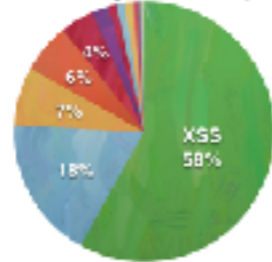
Cross-Site Scripting (XSS)



- 18 Sep 2014 "eBay Under Fire After Cross Site Scripting Attack"
- 16 Sep 2013 "NASDAQ Website Vulnerable to XSS Attacks"
- 26 May 2013 "PayPal vulnerable to cross-site scripting again"



Vulnerability Classes (2014)



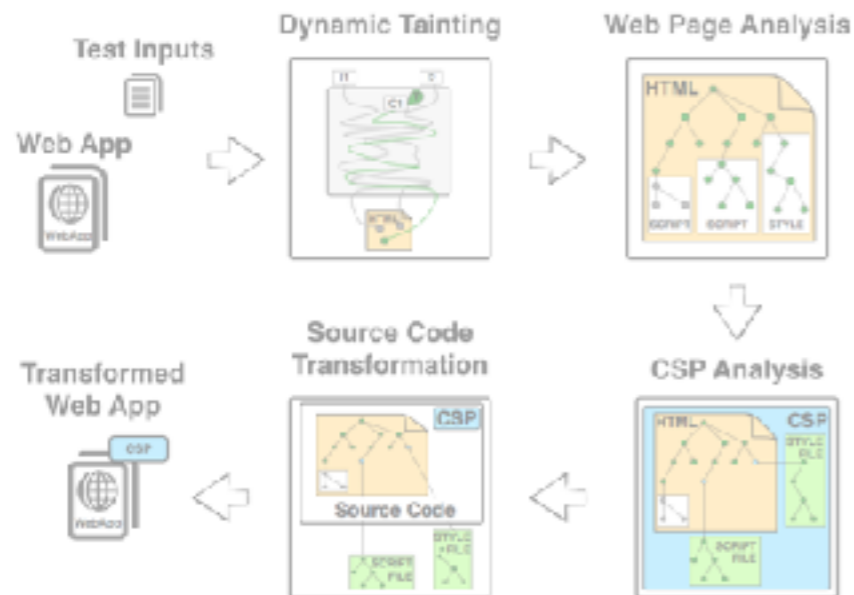
Widfor Security, 2014

Content Security Policy (CSP)

Server CSP Client

11 37 42 8 27

AutoCSP



Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP's performance on the input used for its taint analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?

Summary

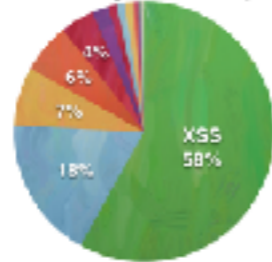
Cross-Site Scripting (XSS)



- 18 Sep 2014 "eBay Under Fire After Cross Site Scripting Attack"
- 16 Sep 2013 "NASDAQ Website Vulnerable to XSS Attacks"
- 26 May 2013 "PayPal vulnerable to cross-site scripting again"



Vulnerability Classes (2014)



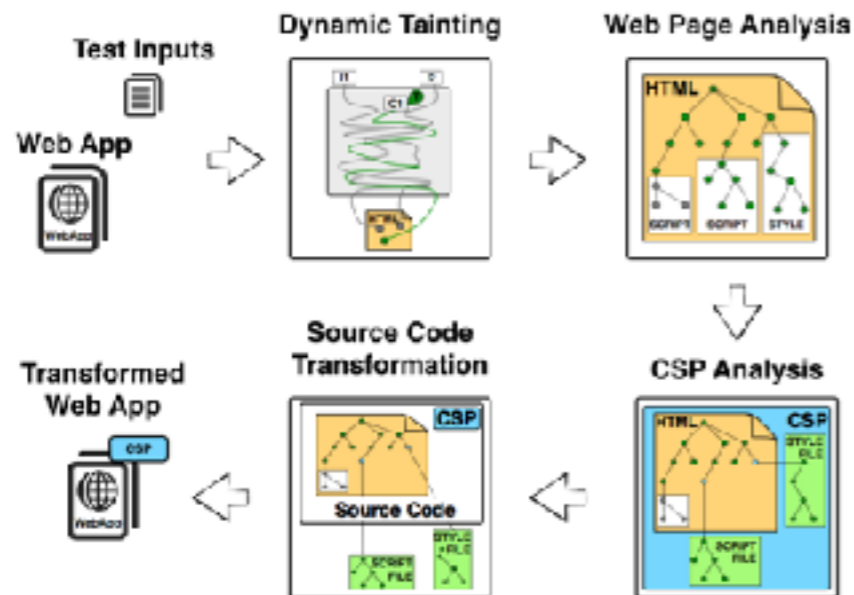
Wired for Security, 2014

Content Security Policy (CSP)

Server CSP Client

11 37 42 8 27

AutoCSP



Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP's performance on the input used for its taint analysis?

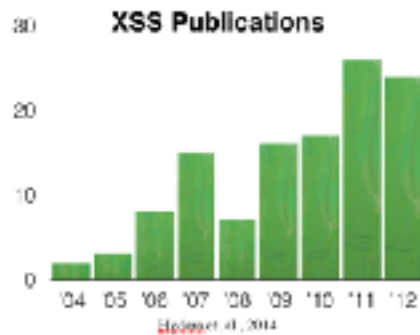
RQ4: Is automation actually needed to retrofit CSP to web applications?

Summary

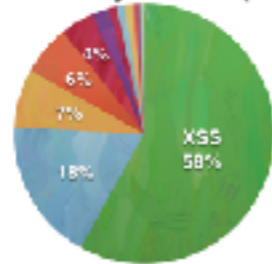
Cross-Site Scripting (XSS)



- 18 Sep 2014 "eBay Under Fire After Cross Site Scripting Attack"
- 16 Sep 2013 "NASDAQ Website Vulnerable to XSS Attacks"
- 26 May 2013 "PayPal vulnerable to cross-site scripting again"



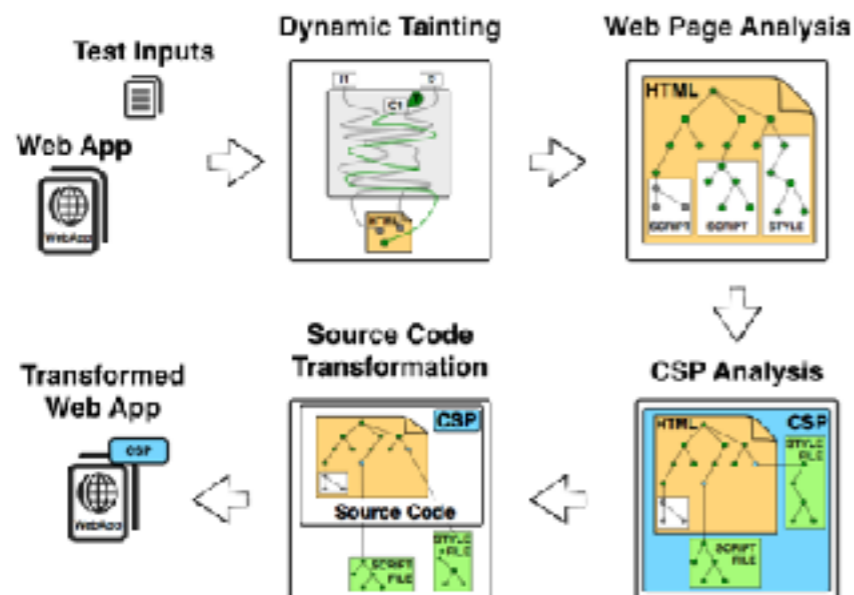
Vulnerability Classes (2014)



Wired for Security, 2014

Content Security Policy (CSP)

AutoCSP



Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications' functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP's performance on the input used for its taint analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?